# COMMUNICATION METHOD, COMMUNICATION SYSTEM, USER TERMINAL ANI COMMUNICATION CONNECTION PROGRAM

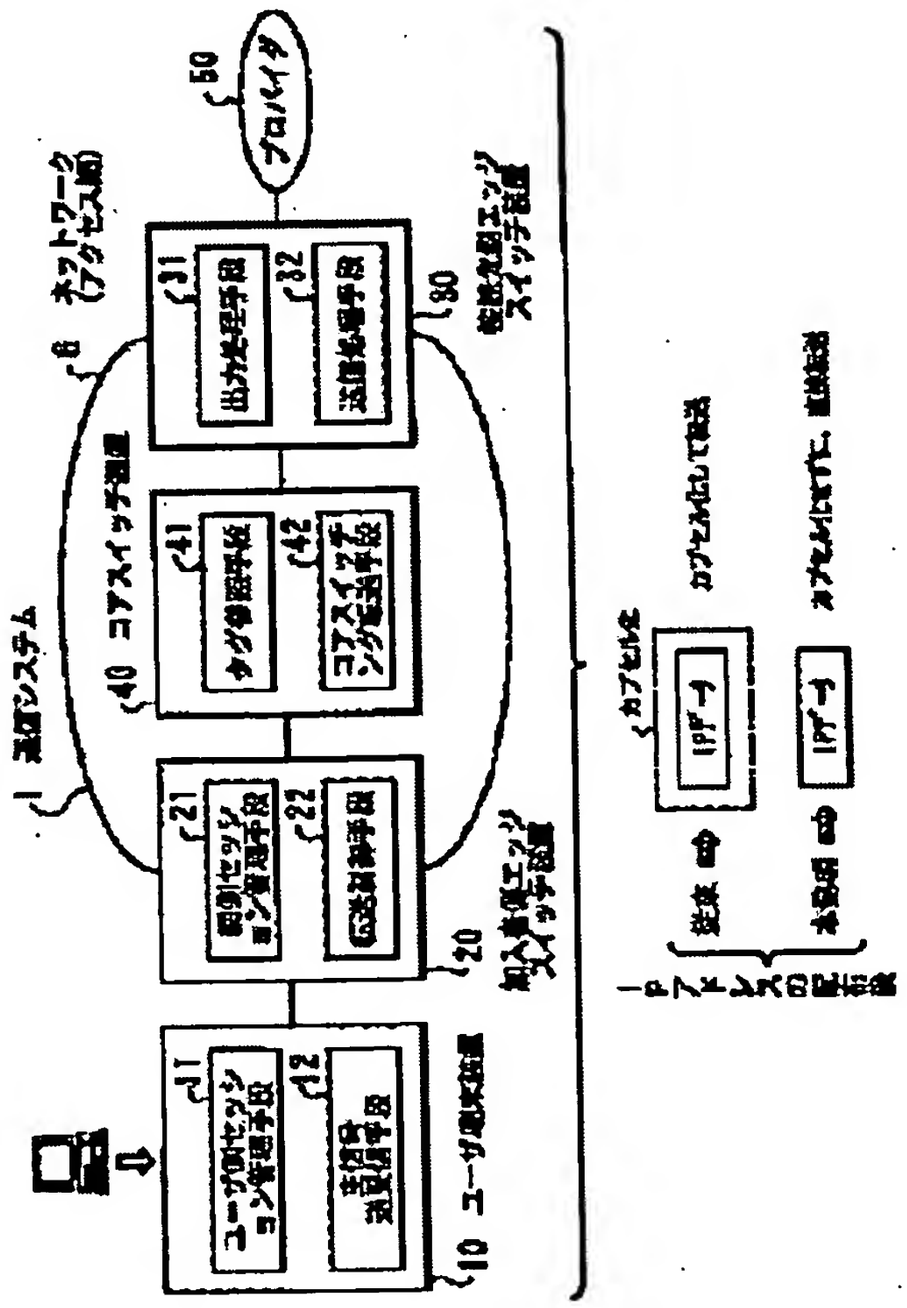
**Publication number:** JP2003060675
**Publication date:** 2003-02-28
**Inventor:** KITADA ATSUSHI; OKUDA MASAHITO
**Applicant:** FUJITSU LTD
**Classification:**
**- international:** ***H04L12/46; H04L29/06; H04L29/12;*** *H04L29/08;* **H04L12/46; H04L29/06; H04L29/12;** H04L29/08; (IPC1-7): H04L12/56; H04L12/46; H04L29/08
**- european:** H04L12/46V; H04L29/06; H04L29/06C6C2; H04L29/12A
**Application number:** JP20010246400 20010815
**Priority number(s):** JP20010246400 20010815

**Also published as:**
US2003037163 (A



Abstract of **JP2003060675**

PROBLEM TO BE SOLVED: To construct a high speed communication system to realize an efficient destination party switching, thereby improving the quality of the communication service. SOLUTION: A user side session control means 11 controls the designation of a destination address, user authentication and IP address allotment at an authentication phase. A main signal transmitting/receiving means 12 transmits/ receives not capsulated main signal frames at a communication phase. A network side session control means 21 performs the signaling control. A transfer control means 22 transfers main signal frames with a tag added for univocally showing a virtual closed network, upon receipt of the signal frames from a user and also transfers main signal frames to a user terminal 10, without the tag, upon receipt thereof from a destination party. An output processing means 31 outputs the main signal frames, without the tag, to the destination party, as the tag corresponds to its output port. A transmission processing means 32 determines the designation party from an input port and transmits a signal with an added tag to the user terminal 10.



W2243

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－60675
(P2003－60675A)
(43)公開日　平成15年２月28日(2003.2.28)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ 12/56 | | Ｈ０４Ｌ 12/56 | Ｈ | ５Ｋ０３０ |
| 12/46 | | 12/46 | Ｖ | ５Ｋ０３３ |
| 29/08 | | 13/00 | ３０７Ａ | ５Ｋ０３４ |

審査請求　未請求　請求項の数10　ＯＬ　（全 43 頁）

(21)出願番号　特願2001－246400(P2001－246400)

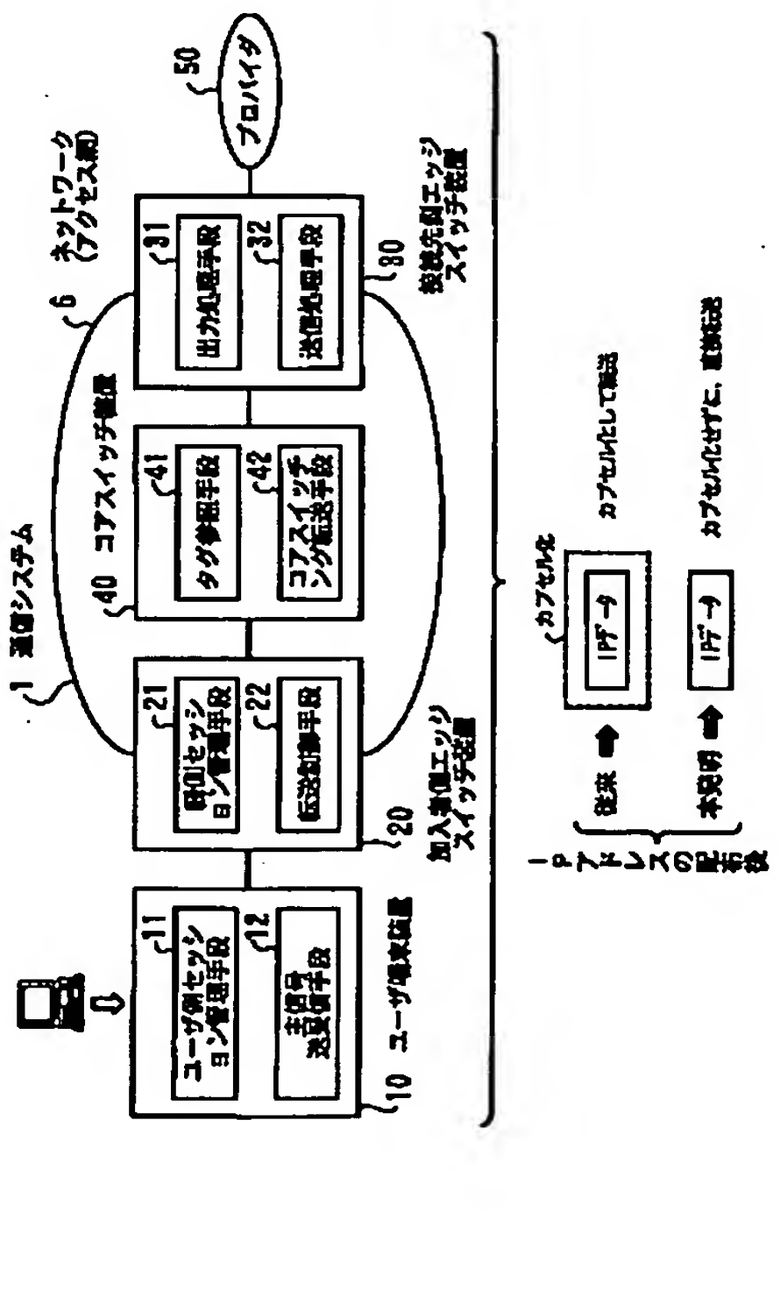
(22)出願日　平成13年８月15日(2001.8.15)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　北田　敦史
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　奥田　將人
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100092152
弁理士　服部　毅巖

最終頁に続く

(54)【発明の名称】　通信方法、通信システム、ユーザ端末装置及び通信接続プログラム

(57)【要約】
【課題】　高速通信可能なシステムを構築して、効率のよい接続先切り替えを実現し、通信サービスの品質の向上を図る。
【解決手段】　ユーザ側セッション管理手段１１は、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての制御を行う。主信号送受信手段１２は、通信フェーズ時に、カプセル化しない主信号フレームを送受信する。網側セッション管理手段２１は、シグナリング制御を行う。転送制御手段２２は、ユーザからの主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先からの受信時には、タグを外してユーザ端末装置１０側へ転送する。出力処理手段３１は、タグと出力ポートとが対応して、タグを外して接続先へ主信号フレームを出力する。送信処理手段３２は、入力ポートより接続先を判断し、タグを付加してユーザ端末装置１０側へ送信する。



【特許請求の範囲】
【請求項１】　ユーザからは、ＩＰｏＥで主信号フレームを送受信し、
前記ユーザでは、レイヤ２レベルで前記主信号フレームと区別可能な制御フレームによって、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、
アクセス網にとっては、接続先仮想閉域網を識別して、送信元ＭＡＣアドレスと、前記接続先仮想閉域網とをマッピングし、
前記アクセス網では、ＭＡＣブリッジングによってレイヤ２レベルの転送を行うことを特徴とする通信方法。
【請求項２】　アクセス網と、
認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、から構成されて仮想閉域網に対するレイヤ２での接続を行うユーザ端末装置と、
を有することを特徴とする通信システム。
【請求項３】　前記制御フレームの受信時には、シグナリング制御を行う網側セッション管理手段と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、前記接続先から転送された主信号フレームの受信時には、前記タグを外して前記ユーザ端末装置側へ転送する転送制御手段と、から構成される加入者側エッジスイッチ装置をさらに有することを特徴とする請求項２記載の通信システム。
【請求項４】　複数の前記接続先と同時接続する場合、前記転送制御手段は、前記ユーザ端末装置及び前記接続先それぞれのレイヤ２アドレスにより、接続先を一意に識別することを特徴とする請求項３記載の通信システム。
【請求項５】　前記タグと出力ポートとが対応して、前記タグを外して前記接続先へ主信号フレームを出力する出力処理手段と、入力ポートより前記接続先を判断し、前記タグを付加して前記ユーザ端末装置側へ送信する送信処理手段と、から構成される接続先側エッジスイッチ装置をさらに有することを特徴とする請求項２記載の通信システム。
【請求項６】　前記加入者側エッジスイッチ装置及び前記接続先側エッジスイッチ装置は、レイヤ２アドレスとレイヤ３アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ２アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ２アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする請求項２記載の通信システム。
【請求項７】　前記ユーザ端末装置からの認証情報の集約、前記認証情報の前記接続先への転送、前記接続先で認証制御された結果を示す認証メッセージの前記ユーザ端末装置への転送、を含む認証に関する一元管理処理を行う通信管理サーバをさらに有することを特徴とする請求項２記載の通信システム。
【請求項８】　前記網側セッション管理手段を前記通信管理サーバに、前記転送制御手段を前記加入者側エッジスイッチ装置に持たせて、前記制御フレームの処理と、前記主信号フレームの処理とを装置的に分離することを特徴とする請求項７記載の通信システム。
【請求項９】　認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、
通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、
を有することを特徴とする、仮想閉域網に対するレイヤ２での接続を行うユーザ端末装置。
【請求項１０】　ユーザ端末装置側に装備され、仮想閉域網に対するレイヤ２での接続を行う通信接続プログラムにおいて、
コンピュータに、
認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、
通信フェーズ時に、カプセル化しない主信号フレームを送受信する、
処理を実行させることを特徴とする通信接続プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信方法、通信システム、ユーザ端末装置及び通信接続プログラムに関し、特にユーザとプロバイダ間の通信サービス実行時の通信制御を行う通信方法、ユーザとプロバイダ間の通信サービス実行時の通信制御を行う通信システム、仮想閉域網に対するレイヤ２での接続を行うユーザ端末装置及びユーザ端末装置側に装備され、仮想閉域網に対するレイヤ２での接続を行う通信接続プログラムに関する。
【０００２】
【従来の技術】インターネット、ディジタルコンテンツ配信など広帯域マルチメディアサービスの普及に伴い、ネットワークの経済的で高速・広帯域なシステムの開発が急速に進められている。
【０００３】例えば、既設の電話用銅線ケーブルを利用して，高速なディジタル伝送を行うＡＤＳＬ（Asymmetric Digital Subscriber Line）や、ユーザ宅に光ファイバケーブルを敷設して、ユーザ端末からより高速・大容量の通信サービスを実現するＦＴＴＨ(Fiber To The Home)などのシステム構築が進められている。

【０００４】また、このようなネットワーク技術の発展に伴って、高画質の映像配信サービスや音楽ダウンロードサービスなどを提供するｘＳＰ(インターネット・サービス・プロバイダやコンテンツ・サービス・プロバイダ等)が、数多く出現すると考えられ、ネットワーク・ビジネス市場の拡大に拍車をかけている。

【０００５】また、近年ではＶＰＮ（Virtual Private Network：仮想閉域網）と呼ばれるネットワーク・サービスが提供されている。これは、社内で構築したネットワークを使って、通信事業者のサービスを、あたかも専用線のように利用できるサービスの総称である。

【０００６】このＶＰＮにより、例えば、社内のＬＡＮをインターネット経由で接続して、仮想的にプライベート・ネットワークを構築することにより、物理的なネットワーク構成に縛られることのない、柔軟で拡張性のあるネットワークを構築することができる。

【０００７】このように、現在のブロードバンド・サービスが広がりつつある状況の中で、ユーザ側では、接続先であるプロバイダを、用途に応じてより柔軟に切り替えたいという要求が高まってきている。

【０００８】一方、ＬＡＮの技術であるイーサネット（Ethernet）（登録商標）がアクセス回線やＷＡＮ回線のテクノロジとして有望視されている（１０Ｇｂ／ｓへの標準化等）。そこで、接続先切り替え機能に必須な、認証／ＩＰアドレス割り当てをイーサネット上で行う方式として、ＰＰＰｏＥ（Point-to-Point Protocol over Ethernet）がある。

【０００９】図６５はユーザとプロバイダとの接続形態を示す図である。図は、ＰＰＰｏＥを利用して、プロバイダへの接続先が切り替え可能な接続形態を示している。イーサネット上のユーザ端末１００は、加入者側の終端装置１１０として、サービス形式がＡＤＳＬならばＡＤＳＬモデムに接続し、ＦＴＴＨならばＯＮＵ（Optical Network Unit）に接続する。ＡＤＳＬモデムやＯＮＵは、ＡＤＳＬ回線またはＦＴＴＨの光回線を通じ、アクセス網６００を介してプロバイダに接続する。

【００１０】ユーザからプロバイダへ接続する際には、ユーザ端末１００は、まず、プロバイダへ発呼し、ユーザＩＤとパスワードを送信する。そして、プロバイダ側で認証されると、ＩＰアドレスが配布されて、その後サービスが開始される。また、接続先の変更は、ユーザＩＤの後に、変更したいプロバイダ名を続けて打ち込んで送信することで、網側がこれを識別して接続先を切り替える。

【００１１】なお、発呼後の一連の処理は、ＰＰＰで実行されるため、ＩＰアドレスの配布には、ＩＰＣＰ（Internet Protocol Control Protocol）が用いられる。ここで、ＰＰＰのレイヤは、ＬＣＰ（Link Control Protocol）とＮＣＰ（Network Control Protocol）の２階層で構成される。ＬＣＰは、上位プロトコルに依存しないデータリンクの確立を実現し、ＮＣＰは、上位プロトコルに依存した処理を受け持つものである。そして、上位プロトコルがＴＣＰ／ＩＰの場合には、ＮＣＰとしてはＩＰＣＰが用いられ、ＩＰＣＰによりＩＰアドレスの決定処理が行われる。

【００１２】図６６はＰＰＰｏＥを利用した従来のネットワークシステムを示す図である。図６５で上述した内容を、ネットワークシステム全体で示した際の概略図である。ユーザ端末１００は、アクセス網６００に接続する（終端装置の図示は省略）。アクセス網６００にはスイッチ部６０１、Ｂ－ＲＡＳ（Broadband Remote Access Server）６１０が設置され、Ｂ－ＲＡＳ６１０は、プロバイダ側のサーバに接続する。

【００１３】このようなシステムに対して、ユーザからプロバイダへ接続する場合、ユーザ端末１００では「ユーザ名@プロバイダ名」と指定し、この情報はスイッチ部６０１を介して、Ｂ－ＲＡＳ６１０へ送信される。Ｂ－ＲＡＳ６１０ではこの情報にもとづいて、接続先のプロバイダに対して、受信したユーザパケットを振り分ける。このような処理によって、ユーザは接続先を任意に選択する。

【００１４】

【発明が解決しようとする課題】しかし、上記のようなＰＰＰｏＥを用いた従来のネットワークシステムでは、Ｂ－ＲＡＳ６１０に処理が集中してしまうために、処理負荷が非常に重く、高速通信アクセス実現の妨げになるといった問題があった。

【００１５】Ｂ－ＲＡＳ６１０に処理が集中する理由としては、例えば、ＩＰ処理をしなければならないため、各ｘＳＰへ接続されるインタフェース毎にＩＰアドレスを設定しなければならず、またユーザとPoint-to-Point接続を行うＰＰＰ仮想インタフェースにもＩＰアドレスが割り振られるため、管理工数がかかってしまうといったことや、異なるｘＳＰに接続する際に、同じユーザなのにセッション管理を行うＢ－ＲＡＳが異なっていると、統計情報や課金などの管理工数がかかってしまうなどといった理由が挙げられる。

【００１６】また、図６６に示したように、ユーザ端末１００からのフレームは、どのプロバイダと接続する場合でも、Ｂ－ＲＡＳ６１０を経由する。そして、ＰＰＰｏＥでは、認証などの制御情報だけでなく、ＩＰパケットなどユーザデータもＰＰＰでカプセル化して転送している。したがって、Ｂ－ＲＡＳ６１０は、すべてのユーザの制御情報だけでなく、プロバイダに転送する主信号までもが集中してしまう。

【００１７】ＰＰＰｏＥにおける制御情報のネゴシエーションは、互いに条件をリクエスト(Configure-Request)し合って、互いに承認(Configure-Ack)しあう必要がある。しかも、ユーザ毎に条件が異なるため、ソフトウェア処理が前提となる。

【００１８】また、プロバイダに転送するためには、Ｂ－ＲＡＳ６１０は、レイヤ３の処理もしなければならず（仮想ルータ機能と呼ばれる）、全インタフェース分（プロバイダ数×加入者数だけのＰＰＰ仮想インタフェース及びプロバイダ側インタフェース）のルーティングテーブルをハンドリングする必要がある。

【００１９】このように、従来では上記のような多岐にわたる処理を、Ｂ－ＲＡＳ６１０がすべて行っていたために、Ｂ－ＲＡＳ６１０がボトルネックとなっており、ＰＰＰｏＥを利用した従来のネットワークシステムでは高速化に限界があった。

【００２０】本発明はこのような点に鑑みてなされたものであり、高速通信可能なシステムを構築して、効率のよい接続先切り替えを実現し、ユーザとプロバイダ間での通信サービスの品質の向上を図った通信方法及び通信システムを提供することを目的とする。

【００２１】また、本発明の他の目的は、効率のよい接続先切り替えを実現し、通信サービスの品質の向上を図ったユーザ端末装置を提供することである。さらに、本発明の他の目的は、効率のよい接続先切り替えを実現し、通信サービスの品質の向上を図った通信接続プログラムを提供することである。

【００２２】

【課題を解決するための手段】本発明では上記課題を解決するために、図１に示すような、本発明の通信方法をもとに構成された通信システム１において、アクセス網６と、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段１１と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段１２と、から構成されてレイヤ２での通信接続を行うユーザ端末装置１０と、制御フレームの受信時には、シグナリング制御を行う網側セッション管理手段２１と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、タグを外してユーザ端末装置１０側へ転送する転送制御手段２２と、から構成される加入者側エッジスイッチ装置２０と、タグと出力ポートとが対応して、タグを外して接続先へ主信号フレームを出力する出力処理手段３１と、入力ポートより接続先を判断し、タグを付加してユーザ端末装置１０側へ送信する送信処理手段３２と、から構成される接続先側エッジスイッチ装置３０と、を有することを特徴とする通信システム１が提供される。

【００２３】ここで、ユーザ側セッション管理手段１１は、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行う。主信号送受信手段１２は、通信フェーズ時に、カプセル化しない主信号フレームを送受信する。網側セッション管理手段２１は、制御フレームの受信時には、シグナリング制御を行う。転送制御手段２２は、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、タグを外してユーザ端末装置１０側へ転送する。出力処理手段３１は、タグと出力ポートとが対応して、タグを外して接続先へ主信号フレームを出力する。送信処理手段３２は、入力ポートより接続先を判断し、タグを付加してユーザ端末装置１０側へ送信する。

【００２４】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は本発明の通信システムの原理図である。本発明の通信方法をもとに構成された通信システム１は、アクセス網６を通じて、ユーザとプロバイダ間の通信サービス実行時の通信制御を行う。

【００２５】ユーザ端末装置１０に対し、ユーザ側セッション管理手段１１は、認証フェーズ時に、制御フレームを用いて、接続先（ｘＳＰ：プロバイダ５０）の指定及びユーザ認証／ＩＰアドレス割り当ての処理を含む制御を行う。

【００２６】主信号送受信手段１２は、通信フェーズ（ＩＰ通信フェーズ）時に、認証フェーズのプロトコルを介さずに、カプセル化しない主信号フレームを直接（レイヤ２で）送受信する。

【００２７】ここで、従来では、ユーザ側の端末が、ＶＰＮサービスを利用して、接続先と通信する場合には、認証からＩＰパケットの送受信までの通信シーケンスをすべてトンネリング・プロトコル（ＩＰパケットに、新しいオーババイトヘッダを付加してカプセル化し、相手先に送信するプロトコル）を用いて通信制御していた。

【００２８】一方、本発明のユーザ端末装置１０では、通信接続シーケンスを、認証フェーズとＩＰ通信フェーズの２つに分け、認証フェーズではＰＰＰｏＥのプロトコルを使用し、通信フェーズではIP over Ethernet(ＩＰｏＥ)を使用してＩＰパケットに対するカプセル化はせずに、ＩＰパケットの送受信を行うものである。

【００２９】加入者側エッジスイッチ装置２０に対し、網側セッション管理手段２１は、制御フレームの受信時に、シグナリング制御を行う。転送制御手段２２は、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、タグを外してユーザ端末装置１０側へ転送する。

【００３０】接続先側エッジスイッチ装置３０に対し、出力処理手段３１は、タグと出力ポートが対応して、接続先へ主信号フレームを出力する（実際には、ｘＳＰ側に割り当てていたポートがアクセス網６側のポートとして動作させたり、その逆の動作を行うようなことも可能）。送信処理手段３２は、入力ポートより接続先を判

断し、タグを付加してアクセス網６を通じて、ユーザ端末装置１０側へ送信する。

【００３１】コアスイッチ装置４０に対し、タグ参照手段４１は、受信した主信号フレームのタグを参照する。コアスイッチング転送手段４２は、レイヤ２レベルで主信号フレームの転送を行う。

【００３２】次にＰＰＰｏＥの従来のＶＰＮシステムに対して、本発明の通信システム１を適用した場合の具体的な構成及び動作について以降詳しく説明する。まず、通信システム１全体の概要について説明する。

【００３３】上述したように、ＰＰＰではユーザ認証及びＩＰアドレスの割り当てを受けて、実際のＩＰデータ通信を行う。このユーザ認証とＩＰアドレス割当の機構は、ｘＳＰ切替接続には必須の機能である。ユーザ認証は当然として、ｘＳＰを切り替えるということはＩＰサブネットが切り替わるということであり、ＩＰｖ６に移行してもサブネットＩＤの割当を受けることは必須である。しかし，ＩＰアドレス割当後、ＩＰデータに関しては、中継アクセス網において、ユーザが正しく認証されていることを確認して、適切に該当ｘＳＰに転送することができれば、ＰＰＰでカプセル化して転送する必要性はない。

【００３４】したがって、本発明では、ＰＰＰｏＥをシグナリングのメカニズムとしてのみとらえ、ＩＰデータに関しては、カプセル化しない主信号を、IP over Ethernet（ＩＰｏＥ）で直接送受信するようにする。

【００３５】すなわち、ユーザがプロバイダと通信する際には、認証フェーズとＩＰ通信フェーズに分けて、各フェーズに対して、レイヤ２レベルで、制御フレームと主信号フレームで認識・処理する。

【００３６】したがって、制御フレーム（ＰＰＰｏＥ）により、ユーザ端末装置１０が発呼して、ユーザ認証及びＩＰアドレス割当のネゴシエーションを行った後（認証フェーズ）、ユーザ端末装置１０からは、割当を受けたＩＰアドレスを設定して、主信号フレームであるＩＰデータ（ＩＰｏＥ）を送出する(ＩＰ通信フェーズ)。

【００３７】ただし、ユーザ端末装置１０と、アクセス網６（加入者側エッジスイッチ装置２０）との接続セッションの維持は、ＰＰＰｏＥのメカニズムを用い、例えば、接続確認（ＬＣＰ：Echo-Request/Reply）や切断処理（ＬＣＰ：Terminate-Request/Ack）等は、ＰＰＰｏＥで送受のやりとりを行う。

【００３８】そして、アクセス網６での、ユーザのセッション管理については、本発明では、ユーザ端末装置１０が接続された、アクセス網６内の加入者側エッジスイッチ装置２０において、送信元ＭＡＣ（Media Access Control）アドレスでユーザのセッションを管理する（なぜなら、制御フレームであるＰＰＰｏＥフレームも、主信号フレームであるＩＰｏＥフレームも、出力するEthernet インタフェースが同じであれば、レイヤ２アドレスである送信元ＭＡＣアドレスは同一であるから）。

【００３９】また、加入者側エッジスイッチ装置２０は、認証フェーズ完了（認証成功及びＩＰアドレス割当完了）後に、認証フェーズ時に受信した「ユーザ名@プロバイダ名」から抽出した接続先のプロバイダと、送信元ＭＡＣアドレス（ユーザ端末装置１０のＭＡＣアドレス）とをマッピングしておく。これにより、送信元ＭＡＣアドレスから接続先プロバイダを認識して、主信号フレームを転送することが可能になる（ＭＡＣアドレスでセッションを識別するので、エッジスイッチ装置のポートに複数端末が接続された環境でも適切にセッションを管理できる）。

【００４０】なお、ここでの制御はＶＬＡＮ（Virtual LAN）技術を応用したものである。ＶＬＡＮとは、入力フレームの伝達範囲を物理的な構成に制限されずに、論理的なネットワークとして構成する技術である。このＶＬＡＮ機能を用いることで、入力フレームのグループを識別して、同一グループに属する端末にのみフレームを送信することができる。

【００４１】また、ＶＬＡＮによる識別制御にはいくつかの種類があり、ここでは、入力フレームの送信元ＭＡＣアドレスから相手を識別する、ＭＡＣアドレスＶＬＡＮを適用している（ただし、従来のＭＡＣアドレスＶＬＡＮは、ユーザのＭＡＣアドレスを静的に登録しておくが、本発明では、認証フェーズで抽出した接続先プロバイダに対応して、後述のテーブル登録により、ＭＡＣアドレスとＶＬＡＮとの対応を動的に切り替え可能とするものである）。

【００４２】一方、加入者側エッジスイッチ装置２０では、主信号フレーム(ＩＰｏＥフレーム)に関して、プロバイダに対応したタグを付加して、アクセス網６を転送する。そして、アクセス網６内のコアスイッチ装置４０では、タグを参照して、接続先プロバイダを一意に識別し（タグ参照手段）、レイヤ３を見ることなく、レイヤ２レベルのＭＡＣブリッジング転送により、主信号フレームの転送を行う（コアスイッチング転送手段）。

【００４３】なお、本発明では、プロバイダを一意に識別するタグとしてIEEE802.1QのＶＬＡＮ－Ｔａｇ（ＶＬＡＮ技術の１つで、４バイトのＶＬＡＮ－Ｔａｇを付加して、このＶＬＡＮ－Ｔａｇからグループ（相手端末）を識別する機能）を用いるが、アクセス網６内でプロバイダを一意に識別できるタグであれば、独自に規定したタグを用いても構わない。

【００４４】このように、本発明ではユーザ端末装置１０と、加入者側エッジスイッチ装置２０とで、シグナリング処理を行い、主信号はＩＰデータのＰＰＰのカプセル化をせずに、アクセス網６内をレイヤ２レベルで、タグを用いたスイッチングで転送する構成にした。

【００４５】これにより、システム内で分散処理が行われるので、従来のような処理負荷が集中するＢ－ＲＡＳ

６１０が不要となり、より柔軟で拡張性に富んだネットワークを構築でき、通信サービスの品質向上を図ることが可能になる。

【００４６】また、本発明の効果として、Ｂ－ＲＡＳのかわりに、エッジスイッチ装置に処理を持たせることにしたので、安価にシステムを構築することができる（すなわち、レイヤ３処理を行うルータのような機器に比べ、安価なＬ２ＳＷ（EtherSW）に拡張機能として本発明の機能を設置させることができるので安価に実現可能）。

【００４７】さらに、レイヤ２レベルのＭＡＣブリッジングで転送するため、アドレス学習は自動で行われ、管理工数の削減を図ることが可能になる（各インタフェース毎にＩＰアドレスの設定も不要）。また、ユーザのセッション管理は、異なるｘＳＰ接続の場合でも、加入者側エッジスイッチ装置（または、後述の通信管理サーバ）で行うことができる。

【００４８】なお、加入者側エッジＬ２ＳＷの加入者側１ポートあたり１ユーザしか接続しない構成であれば、必ずしも（動的）ＭＡＣアドレスＶＬＡＮである必要はなく、（動的）ポートＶＬＡＮ、すなわち認証フェーズ完了後に入力ポートと接続先仮想閉域網をマッピングする方式でも構わない。

【００４９】次に本発明を適用した際の他の効果として、ＩＰフラグメント処理を不要とできる旨について説明する。まず、ＩＰｏＥのＩＰパケットの最大長（ＭＴＵ：Maximum Transfer Unit）は１５００バイトである。一方、従来のＰＰＰｏＥでは、ＩＰパケットをＰＰＰでカプセル化して転送するため、８バイトのオーバヘッドが生じる。したがって、この８バイトのオーバヘッド分、ＩＰパケット部分が短くなるので、ＰＰＰｏＥのＩＰパケットのＭＴＵは、１４９２バイトとなる。

【００５０】ここで、従来、ユーザからの上り通信の場合では、ＬＣＰでＩＰパケットのＭＴＵを１４９２バイトとしてネゴシエーションしているために、フラグメント処理は回避されていた。

【００５１】ところが、網側からの下りフレーム（インターネット等からの下りフレーム）は、EthernetでのＭＴＵである１５００バイトで送られてくる場合があり、この場合には、Ｂ－ＲＡＳ６１０やプロバイダ側のルータでは、ＰＰＰｏＥのカプセル化を実行するために、ＩＰのフラグメント処理を施す必要があった。

【００５２】フラグメント処理は、一般に負荷の重い処理である。このため、通常の通信制御でも高負荷であったＢ－ＲＡＳ６１０に対し、さらにフラグメント処理が加わってしまうと、さらに効率が低下してしまうことになる（なお、フラグメント禁止フラグがセットされたりすると、フラグメントできないＩＰパケットは、廃棄されてしまうため、通信の信頼性の低下を引き起こすことになる）。

【００５３】図２はフレーム構成を示す図である。（Ａ）は改正前、（Ｂ）は改正後、（Ｃ）はＰＰＰｏＥでカプセル化した場合のフレーム構成を示している。

（Ａ）のフレームは、IEEE802.3委員会での改正前のＩＰデータフレームの構成である。ヘッダが１４バイト、ＩＰパケットのＭＴＵは１５００バイト、ＦＣＳ（フレームチェックシーケンス）は４バイトであり、改正前の最大フレーム長は１５１８バイトであった。

【００５４】（Ｂ）のフレームは、IEEE802.3委員会での改正後のＩＰデータフレームであり、（Ａ）のヘッダ部分が４バイト伸びて、最大フレーム長が改正前の１５１８バイトから１５２２バイトに改正されている(IEEE802.3ac-1998)。なお、（Ｂ）のフレームは、タグを付加した際の本発明の主信号フレームの構成を表している。

【００５５】すなわち、（Ｂ）のフレームは、ヘッダ１４バイト、IEEE802.1Qで規定されたＶＬＡＮ－Ｔａｇが４バイト、ＩＰパケットのＭＴＵは１５００バイト、ＦＣＳは４バイトで構成され、最大フレーム長は１５２２バイトである。

【００５６】このように、改正後では、ＩＰパケットのＭＴＵが１５００バイトのままで、４バイトのタグを付加できる。このため、本発明に対しては、フラグメント処理は発生しない。

【００５７】一方、（Ｃ）のフレームは、改正後のフレームをＰＰＰｏＥでカプセル化した場合を示している。図に示すように、ＰＰＰｏＥでカプセル化する場合は、改正後でフレーム長が伸びた場合でも、８バイトのオーバヘッド部分は、ペイロードに含まれることになるので、ＩＰパケットのＭＴＵは、１４９２バイトで変わりはない。したがって、ＰＰＰｏＥで通信を行えば、フラグメント処理が発生してしまう可能性がある。

【００５８】以上説明したように、本発明では、主信号フレームのＭＴＵサイズは、ＩＰｏＥの１５００バイトで送受信することができるので、フラグメント処理は発生せず、効率のよい通信制御を行うことが可能になる。

【００５９】次に通信システム１の具体的な構成について説明する。図３は通信システム１の構成例を示す図である。アクセス網６のユーザ側のエッジ部分には、加入者側エッジスイッチ装置（以下、加入者側エッジＬ２ＳＷ（layer2 switch））２０－１、２０－２が配置され、接続先であるプロバイダ側のエッジ部分には、接続先側エッジスイッチ装置（以下、プロバイダ側エッジＬ２ＳＷ）３０－１、３０－２が配置される。また、アクセス網６内部には、コアスイッチ装置（以下、コアＬ２ＳＷ）４０－１、４０－２とProxy Radiusサーバ（通信管理サーバに該当）６１が配置されて、図のように接続されている。

【００６０】また、ユーザ端末装置１０－１、１０－２は、加入者側エッジＬ２ＳＷ２０－１に接続し、ユーザ端末装置１０－３は、加入者側エッジＬ２ＳＷ２０－２

に接続する。プロバイダ側エッジＬ２ＳＷ３０－１、３０－２は、それぞれのＩＳＰが有するプロバイダエッジルータ５１－１、５１－２に接続し、プロバイダエッジルータ５１－１、５１－２にはプロバイダRadiusサーバ５２－１、５２－２がそれぞれ接続する。

【００６１】なお、Radius（Remote Authentication Dial-in User Service）とは、認証機構をネットワークに導入する際に用いられる代表的なプロトコルのことであり（ＲＦＣ２８６５で規定されている）、このRadius機能を含むサーバやクライアントをRadiusサーバ、Radiusクライアントと呼ぶ。

【００６２】図４は主信号フレームのフォーマットを示す図である。認証フェーズ完了後、ユーザ端末装置１０から送信される主信号フレームのフォーマットを示している。

【００６３】図２の（Ｂ）に対応させると、１４バイトのEtherヘッダの部分がDESTINATIONADDR（６バイト）、SOURCE ADDR（６バイト）、ETHER TYPE（２バイト）に該当する。そして、その他のフィールドは、ＩＰパケットに含まれる。

【００６４】また、ETHER TYPEはフレームタイプを示すものであり、０ｘ０８００ならば、このフレームは主信号フレームであることを示し、０ｘ８８６３（PPPoE Discovery Stage用フレーム）または０ｘ８８６４（PPPoE Session Stage用フレーム）ならば制御フレームであることを示す。

【００６５】認証フェーズ完了後、このような主信号フレームを加入者側エッジＬ２ＳＷ２０が受信すると、送信元ＭＡＣアドレス（上述のSOURCE ADDR）から接続先のプロバイダを識別し、加入者側エッジＬ２ＳＷ２０はタグを付加して転送する。なお、受信した送信元ＭＡＣアドレスがマッピングされていなければ、そのユーザからのフレームは廃棄する。これにより、認証が行われていないユーザからの不正アクセスなどは回避できる。

【００６６】図５は主信号フレームのフォーマットを示す図である。タグが付加されたときの主信号フレームのフォーマットを示している。図２の（Ｂ）に対応させると、１４バイトのEtherヘッダの部分がDESTINATION ADDR（６バイト）、SOURCE ADDR（６バイト）、ETHER TYPE（２バイト）に該当し、４バイトのIEEE802.1QのＶＬＡＮ－Ｔａｇの部分が、ＴＰＩＤ（２バイト）、ＰＲＩ（３ビット）、ＣＦＩ（１ビット）、ＶＩＤ（１２ビット）に該当する。また、ETHER TYPEが０ｘ０８００で、TPIDが０ｘ８１００のとき、タグ付き主信号フレームであることを示し、ＶＩＤフィールドから識別する。

【００６７】ここで、タグが付加された主信号フレームは、アクセス網６内のコアＬ２ＳＷ４０でスイッチングされて、プロバイダ側エッジＬ２ＳＷ３０まで転送されると、プロバイダ側エッジＬ２ＳＷ３０でタグが外されて、指定のプロバイダへ到着することになる。逆に、プロバイダからユーザへの下りフレームは、ポートベースのＶＬＡＮにより（すなわち、プロバイダ側エッジＬ２ＳＷ３０のポートに対応してＶＩＤのタグを設定している。後述する。）、上りのときと同様にタグを付加して、アクセス網６内を転送する。

【００６８】このように、本発明では、ＩＰパケットをレイヤ２レベルでセキュアに（安全に）プロバイダへ転送することが可能である。そして、レイヤ２レベルで転送することのメリットとしては、将来ＩＰｖ６に移行した場合にも、レイヤ３を見ることなく、ETHER TYPEで主信号であることを判別して転送可能なため、アクセス網６内の装置を変更する必要がない。なお、ＩＰｖ６のETHER TYPEは、０ｘ８６ＤＤである。

【００６９】また、本発明の通信システム１の効果として、図３のような構成にすることにより、既存設備をほとんど変更なく流用可能な点を挙げることができる。図３に示す構成に対し、加入者側エッジＬ２ＳＷ２０にRadiusクライアントを搭載し、アクセス網６に設置したProxy Radiusサーバ６１で一旦認証情報を集約し、Proxy Radiusサーバ６１から各プロバイダRadiusサーバ５２に転送する方式をとれば、プロバイダエッジルータやプロバイダRadiusサーバの設定／データベース及び管理運用をほとんど変更なく使用できる。

【００７０】また、アクセス網６のコアＬ２ＳＷ４０は、タグを識別してフレームをＭＡＣブリッジング転送できればよく、IEEE802.1Q ＶＬＡＮ－Ｔａｇを用いるのであれば、市販で手に入るようなIEEE802.1Q対応のスイッチ装置を活用することができるので、容易にネットワークを構築することが可能である。

【００７１】なお、本発明では、シグナリングのメカニズムとしてＰＰＰｏＥを取り上げているが、必ずしもＰＰＰｏＥに限定したものではなく、例えばIEEE802.1Xをポート単位の認証ではなく、ユーザ(ＭＡＣアドレス)単位の認証ととらえ、ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバと密接に連携して、ＩＰアドレスの割当及び解放動作を適切に行えば、ＰＰＰｏＥに代わるシグナリングメカニズムとして本発明において適用できる。

【００７２】ここで、IEEE802.1X（Port Based Network Access Control）は、イーサネット上でポート単位のアクセスコントロールを行う方式であるが、ポート単位なので１ポートに複数端末が接続された環境では使用できない。ただし、ネゴシエーション中で送信元ＭＡＣアドレスより相手装置を特定できるので、ポート単位ではなく、送信元ＭＡＣアドレス単位でのアクセスコントロールととらえることにより複数端末にも対応可能である。

【００７３】また、IEEE802.1Xは、ＩＰアドレス割り当てのメカニズムを備えていない。一般には、ＤＨＣＰ（別プロトコル）によってＩＰアドレスが割り当てられ

る。したがって、本発明で適用する場合、ユーザがどのＩＰアドレスを使用しているか、またｘＳＰを切り替える際などは、ＩＰアドレス解放を適切に行うことが必要である（ＤＨＣＰは一般にリースを受けたＩＰアドレスを継続使用しようとする）。

【００７４】次に本発明の認証フェーズ時のシーケンスについて説明する。図６は認証フェーズ時のシーケンスを示す図である（なお、ＩＰ通信フェーズのシーケンスは図３３、３４に示す）。なお、Proxy Radiusサーバ６１を用いて、認証に関する情報の中継制御を行った場合の動作シーケンスである（Proxy Radiusサーバ６１の詳細は後述する）。

【００７５】認証フェーズ時のＰＰＰｏＥは大きく、PPPoE Discovery StageとPPP SessionStageに分かれる。また、ユーザ端末装置１０のユーザ側セッション管理手段１１と、加入者側エッジＬ２ＳＷ２０の網側セッション管理手段２１とで、認証フェーズの通信制御を行う。なお、以下は、ＰＰＰｏＥのシグナリングメカニズムを例としたシーケンスである。

【００７６】〔Ｓ１〕ユーザ側セッション管理手段１１と網側セッション管理手段２１間でＰＡＤＩ（PPPoE Active Discovery Initiation）、ＰＡＤＯ（PPPoE Active Discovery Offer）、ＰＡＤＲ（PPPoE Active Discovery Request）を送受信する。そして、網側セッション管理手段２１から送信されたＰＡＤＳ（PPPoE ActiveDiscovery Session-confirmation）を、ユーザ側セッション管理手段１１が受信することで、セッションＩＤが確立する。

【００７７】〔Ｓ２〕ＬＣＰによりデータリンクが確立する。

〔Ｓ３〕網側セッション管理手段２１からCHAP（Challenge Handshake Authentification Protocol） CHALLENGEが送信され、ユーザ側セッション管理手段１１は、CHAP RESPONSEを返信する。CHAP RESPONSEには、ユーザ名@プロバイダ名、パスワードが含まれる。なお、CHAPとは、パスワードを暗号化してネットワークに送信する認証プロトコルのことである。

【００７８】〔Ｓ４〕網側セッション管理手段２１は、認証情報であるRadius Access-Request（ユーザ名@プロバイダ名、パスワード、CHAP CHALLENGE等を含む）をProxyRadiusサーバ６１に送信し、Proxy Radiusサーバ６１は、プロバイダRadiusサーバ５２へRadius Access-Requestを中継する。

〔Ｓ５〕プロバイダRadiusサーバ５２は、認証が成功すると（このように、実際の認証はプロバイダRadiusサーバ側で行われる）、Proxy Radiusサーバ６１にRadius Access-Accept（ユーザ割当用のＩＰアドレス、対向（通信相手）のＩＰアドレス等を含む）を送信し、Proxy Radiusサーバ６１は、網側セッション管理手段２１へRadius Access-Acceptを中継する。

【００７９】〔Ｓ６〕網側セッション管理手段２１は、Radius Access-Acceptを受信するとCHAP SUCCESSをユーザ側セッション管理手段１１へ送信する。

〔Ｓ７〕ユーザ側セッション管理手段１１と網側セッション管理手段２１は、ＩＰＣＰにより、Radius Access-Acceptの受信値をもとに、ＩＰアドレスネゴシエーションを行う。このＩＰＣＰの完了後にＩＰ通信フェーズへ移行する。

【００８０】次に加入者側エッジＬ２ＳＷ２０について説明する。図７～図１０は加入者側エッジＬ２ＳＷ２０が有するテーブルを示す図である。図７のテーブルは、認証フェーズ時に参照する、ユーザの送信元ＭＡＣアドレスとユーザのセッションＩＤの対応が示されるセッション管理テーブルＴ２ａであり、図８のテーブルは、ＩＰ通信フェーズ時に参照する、ユーザのＭＡＣアドレスと接続先プロバイダ毎のタグとの対応が示されるＶＩＤテーブルＴ２ｂである。

【００８１】なお、本発明でいうところのＶＬＡＮ－ＩＤとは、仮想閉域網を一意に示すタグのことであり（ＶＩＤとも表記）、以降では、加入者側エッジＬ２ＳＷが参照するＶＩＤテーブルをＭＡＣ－ＶＩＤテーブル、プロバイダ側エッジＬ２ＳＷが参照するＶＩＤテーブルをポートＶＩＤテーブルと呼ぶ。

【００８２】また、図９のテーブルは、ＶＬＡＮ－ＩＤ毎に（プロバイダ毎に）独立したフォワーディング情報（転送情報）からなるフォワーディングテーブルＴ２ｃであり、図１０のテーブルは、加入者側エッジＬ２ＳＷ２０に設置されている各ポートの属性を示すポート属性テーブルＴ２ｄである。

【００８３】セッション管理テーブルＴ２ａは、（送信元）ＭＡＣアドレス（ユーザ端末装置１０のＭＡＣアドレス）、セッションＩＤ、状態及びユーザに割り当てるＩＰアドレス等のネゴシエーションパラメータの項目から構成され、認証フェーズの時に用いるテーブルである。

【００８４】セッションＩＤは、図６で上述したPPPoE Discovery Stageにおいて確立するＩＤ（２バイト）を示し、状態は、認証フェーズか、またはＩＰ通信フェーズであるかのいずれかの現在の通信状態を示す。また、ネゴシエーションパラメータは、エッジＬ２ＳＷにユーザごとにあらかじめ登録しておくものではなく、例えば、ユーザに割り当てるＩＰアドレスなどは各ｘＳＰより指定され、仮想閉域網を一意に示すＶＩＤは、ＶＩＤ情報を一元管理する通信管理サーバより指定される。

【００８５】ＭＡＣ－ＶＩＤテーブルＴ２ｂは、（送信元）ＭＡＣアドレスとセッションＩＤ及びＶＬＡＮ－ＩＤの項目から構成され、ＩＰ通信フェーズの時に用いるテーブルである。なお、図では、セッション管理テーブルＴ２ａとＭＡＣ－ＶＩＤテーブルＴ２ｂとを、別々のテーブルで構成しているが、１つのテーブルで構成して

もよい。
【００８６】フォワーディングテーブルＴ２ｃは、（宛先）ＭＡＣアドレスと、加入者側エッジＬ２ＳＷ２０が持つ出力ポートの項目から構成され、アドレス学習及びエージングによりエントリ（テーブル内容）が追加・削除される。
【００８７】また、フォワーディングテーブルＴ２ｃは、プロバイダ（ＶＬＡＮ－ＩＤ）毎に独立している。このため、１つの（宛先）ＭＡＣアドレスから異なるプロバイダに出力することを防ぎ、不要なテーブル検索を抑制することが可能である。
【００８８】ポート属性テーブルＴ２ｄは、ポート番号、受信フレーム、ブロードキャストフィルタリング及びタグ挿抜の項目から構成されて、ポート属性が示されるテーブルである。
【００８９】加入者側エッジＬ２ＳＷ２０へのポート入力時には、受信フレームの欄を見て、そのフレームを受け入れてよいか確認し、ポート出力時には、ブロードキャストフィルタリング及びタグ挿抜の欄を見て、どのような形式でフレームを出力するかを決定する。
【００９０】ここで、図に示すポート属性テーブルＴ２ｄに対し、ポート番号１～４のポートがユーザ端末装置１０側に接続するポートであり、ポート番号５～７のポートがアクセス網６側に接続するポートであるとする。この場合例えば、１番のポートでは、入力フレームがＰＰｏＥ、ＩＰ、ＡＲＰ（Address Resolution Protocol）のいずれかのフレームであればそのフレームを取り込むことを表している（ＡＲＰ処理については後述）。
【００９１】また、５番のポートではIEEE802.1Q（すなわち、タグ付きフレーム）、ＧＶＲＰ、ＳＴＰのいずれかのフレームであれば、そのフレームを取り込むことになる。
【００９２】一方、ポート出力に対して、１番のポートからフレームを出力する場合には、ユーザ端末装置１０側へフレーム出力することになるので、ブロードキャストフィルタリングをＯＮ（ブロードキャストしない）、タグはＵｎＴａｇ（タグを外す）に設定し、また、５番のポートからフレームを出力する場合には、アクセス網６側へフレーム出力することになるので、ブロードキャストフィルタリングをＯＦＦ（ブロードキャストする）、タグはＷｉｔｈ Ｔａｇ（タグの付加）に設定する。
【００９３】ただし、プロバイダのポリシーによっては、ブロードキャストもユーザに届けたいという場合があり、ユーザ側ポートのブロードキャストフィルタリングをＯＮにしてもよい。
【００９４】ここで、ポート属性テーブルＴ２ｄの受信フレームの欄に、ＧＶＲＰ（GARP VLAN Registration Protocol）、ＳＴＰ(Spanning Tree Protocol)というプロトコル名があるが、ＧＶＲＰはEthernetネットワークにおける、動的なＶＬＡＮ構成情報を通知するプロトコルであり、ＳＴＰはフレームのループを防ぐレイヤ２レベルで動作するEthernet 制御プロトコルのことである。
【００９５】このＧＶＲＰやＳＴＰは、宛先ＭＡＣアドレスとして特別なマルチキャストアドレス（GVRP：01-80-C2-00-00-21、STP：01-80-C2-00-00-00）を用いるので、アクセス網６内でＧＶＲＰやＳＴＰを動作させるのであれば、図１０のようにポート属性テーブルＴ２ｄの該当ポート欄に記入して、マルチキャストアドレスを受け入れ可能に設定しておけばよい。
【００９６】図１１は加入者側エッジＬ２ＳＷ２０の動作概要を示す図である。加入者側エッジＬ２ＳＷ２０は、ポート＃１～＃７を有し、ポート＃１～＃４がユーザ端末装置１０－１～１０－４にそれぞれ接続し、ポート＃５～＃７がアクセス網６側に接続する。また、ユーザ端末装置１０－１～１０－４のそれぞれのＭＡＣアドレスはＡ～Ｄとする。
【００９７】ここで、ユーザ端末装置１０－１は、ＭＡＣアドレス＝ＸのＩＳＰと接続中（ＩＰ通信フェーズ）である状態を示している。上述した各テーブルでこの状態を見ると、まず、ＭＡＣ－ＶＩＤテーブルＴ２ｂより、（送信元）ＭＡＣアドレス＝Ａならば、ＶＬＡＮ－ＩＤ＝１０であり、フォワーディングテーブルＴ２ｃにより、プロバイダ側への（宛先）ＭＡＣアドレス＝Ｘはポート＃５から出力されることがわかる（タグ＝１０（ＶＬＡＮ－ＩＤ＝１０）が付加されてポート＃５から出力される）。
【００９８】ユーザ端末装置１０－２は、ＭＡＣアドレス＝ＹのＩＳＰと接続中である状態を示している。上述した各テーブルでこの状態を見ると、フォワーディングテーブルＴ２ｃにより、ユーザ側への（宛先）ＭＡＣアドレス＝Ｂはポート＃２から出力されることがわかる（タグ＝１１（ＶＬＡＮ－ＩＤ＝１１）が外されてポート＃２から出力される）。
【００９９】ユーザ端末装置１０－３は、ＭＡＣアドレス＝ＺのＩＳＰと接続トライアル中（認証フェーズ）である状態を示している。この段階では、セッション管理テーブルＴ２ａを用いて、ＰＰＰｏＥの接続制御が行われる。
【０１００】また、ユーザ端末装置１０－４は、ＭＡＣアドレス＝ＹのＩＳＰとの接続中にＩＰＸ（Internet Packet Exchange）フレームを送信しようとしている状態を示している。この場合、ポート属性テーブルＴ２ｄでは、ポート＃４の受信フレームの欄にＩＰＸは設定されていないので、ＩＰＸフレームは、加入者側エッジＬ２ＳＷ２０で受け入れられないことになる。
【０１０１】次に加入者側エッジＬ２ＳＷ２０のブロック構成及び動作フローについて説明する。図１２は加入者側エッジＬ２ＳＷ２０のブロック構成を示す図であ

る。加入者側エッジＬ２ＳＷ２０の処理は、フレーム入力処理、フォワーディング処理、フレーム出力処理に大きく分かれる。

【０１０２】フレーム入力処理では、フレーム入力時、まずETHER－TYPE抽出手段２０１はフレームタイプを識別し（また、TPIDからタグ付きか否かも識別する）、ポート属性テーブルＴ２ｄをチェックする。このとき、入力を認めないフレーム(例えば、ＩＰＸフレームなど)であれば廃棄する。

【０１０３】そして、ＰＰＰｏＥのフレームであれば、ＣＰＵ２０２に渡して、セッション管理テーブルＴ２ａをもとにＰＰＰネゴシエーションを行う（ＲＦＣ１６６１で規定された状態遷移図にしたがったネゴシエーションを行う。この状態遷移に関する内容は省略する）。

【０１０４】また、認証フェーズ完了後のＩＰ通信フェーズ接続開始の状態であれば、ＣＰＵ２０２は、ユーザのＭＡＣアドレスを該当プロバイダのＭＡＣ－ＶＩＤテーブルＴ２ｂに登録し、接続終了であれば、ＭＡＣ－ＶＩＤテーブルＴ２ｂより削除する。

【０１０５】そして、入力フレームが、IEEE802.1Qのタグが付加されてないフレームであれば、ＶＬＡＮ－ＩＤチェック手段２０４は、ＭＡＣ－ＶＩＤテーブルＴ２ｂからユーザの接続先プロバイダに対応したＶＬＡＮ－ＩＤを抽出する。もし、ＭＡＣ－ＶＩＤテーブルＴ２ｂにエントリがなければ、そのユーザは未認証等でＩＰ通信フェーズではないとみなしフレームを廃棄する。

【０１０６】一方、IEEE802.1Qフレーム（タグ付きフレーム）の場合は、ETHER－TYPE抽出手段２０１は、ＶＩＤフィールドからＶＬＡＮ－ＩＤを認識し、ペイロード抽出手段２０３は、IEEE802.1Qタグフレームを受信した場合、ETHER-TYPEを抽出し、０ｘ０８００や０ｘ８６ＤＤであれば主信号フレームなのでそのままフォワーディング処理へ、０ｘ０８０６のＡＲＰなどの場合は、ＣＰＵ２０２へ回す。

【０１０７】フォワーディング処理の出力ポート決定手段２０５では、宛先ＭＡＣアドレスにしたがって、ＶＬＡＮ－ＩＤ毎に独立したフォワーディングテーブルＴ２ｃから出力ポートを決定する。この際、送信元ＭＡＣアドレス及び入力ポートからアドレス学習及び一定時間後にエージングを行う。

【０１０８】もし、宛先ＭＡＣアドレスが自分宛て(例えばProxy Radiusサーバ６１からのRadius Access-Acceptなどが該当)であれば、ＣＰＵ２０２に回して処理を行う。フレーム出力処理の出力処理手段２０６では、再度、ポート属性テーブルＴ２ｄにしたがって、タグの挿抜及びブロードキャストフレーム出力の可／不可を決定してフレームを出力あるいは廃棄したり、ユニキャストのフラッディングのフィルタリングを行う。

【０１０９】このように、加入者側エッジＬ２ＳＷ２０では、受信フレームに対し、ETHER－TYPEを見て、制御フレームであるか主信号フレームであるかを判断し、制御フレームならばＣＰＵ２０２に回して処理し、主信号フレームならば、ハードウェアで処理することにより、高速なＩＰデータ通信が可能である。

【０１１０】図１３は加入者側エッジＬ２ＳＷ２０の全体動作を示すフローチャートである。なお、ステップＳ１２はソフトウェア処理、ステップＳ１１とステップＳ１３～ステップＳ１８はハードウェア処理である。

〔Ｓ１１〕ETHER－TYPEを抽出し、抽出した値にもとづき、ステップＳ１２～ステップＳ１５のいずれかへ行く。

【０１１１】〔Ｓ１２〕ＰＰＰｏＥならばＰＰＰｏＥネゴシエーションを行う。

〔Ｓ１３〕ポート属性にない場合は廃棄する。

〔Ｓ１４〕ＩＰｏＥならば送信元ＭＡＣアドレスよりＭＡＣ－ＶＩＤテーブルＴ２ｂを引く。エントリにあればステップＳ１８へ、なければステップＳ１６へ行く。

【０１１２】〔Ｓ１５〕タグ付きフレームならば、ＶＩＤフィールドより、ＶＬＡＮ－ＩＤを認識する。

〔Ｓ１６〕エントリにないので廃棄する。

〔Ｓ１７〕ペイロードを抽出する。

〔Ｓ１８〕フォワーディング処理／出力処理を行う。

【０１１３】図１４は加入者側エッジＬ２ＳＷ２０のＰＰＰｏＥネゴシエーションの動作を示すフローチャートである。

〔Ｓ２１〕ＰＰＰｏＥのフレームを受信すると、送信元ＭＡＣアドレスより、セッション管理テーブルＴ２ａを引く。

〔Ｓ２２〕ＲＦＣ１６６１で規定された状態遷移にしたがって、ユーザに返信またはProxy Radiusサーバ６１へRadius Access-Requestを送信する。

【０１１４】〔Ｓ２３〕新しい状態（State）をチェックする。接続終了ならばステップＳ２４へ、ＩＰ通信フェーズならばステップＳ２５へ、その他ならば終了する。

〔Ｓ２４〕ＭＡＣ－ＶＩＤテーブルＴ２ｂから該当エントリを削除する。

〔Ｓ２５〕ＭＡＣ－ＶＩＤテーブルＴ２ｂへ該当エントリを登録する。

【０１１５】図１５は加入者側エッジＬ２ＳＷ２０のフォワーディング処理／出力処理の動作を示すフローチャートである。

〔Ｓ３１〕フォワーディング処理時、該当のＶＬＡＮ－ＩＤのフォワーディングテーブルＴ２ｃを検索する。

〔Ｓ３２〕エントリが存在するか否かを判断する。あればステップＳ３３へ、なければステップＳ３４へ行く。

【０１１６】〔Ｓ３３〕ポート属性テーブルＴ２ｄにもとづいてタグ挿抜を行う。そして、フレームを出力する。

〔Ｓ３４〕入力ポート以外の各ポートでポート属性テー

ブルＴ２ｄより、ブロードキャストフィルタリング処理を行う。
〔Ｓ３５〕フィルタリングがＯＮならば廃棄する。
【０１１７】次にユーザ端末装置１０について説明する。図１６はユーザ端末装置１０の構成を示す図である。なお、図におけるＩＰ層及びその上位層、またＭＡＣ層に関しては、既存のプロトコルスタックをそのまま使用可能である（本発明の主信号送受信手段１２は、ＴＣＰ層、ＩＰ層、ＭＡＣ層を通じての処理である）。また、図１７には従来のユーザ端末におけるプロトコルスタックを示す。
【０１１８】プロバイダへの接続開始時、まず、ユーザ側セッション管理手段１１より、図６で上述したPADIパケット(PPPoE Active Discovery Initiationにおいて、接続開始時に使用)を送出する(認証フェーズ完了までは、通常のＰＰＰｏＥ動作と同じ)。以降、ユーザ側セッション管理手段１１が持つユーザ側セッション管理テーブル(図１８に例を示す)を参照して、ネゴシエーションを行い、ユーザ認証では、ユーザが接続するプロバイダをユーザＩＤが「ユーザ名@プロバイダ名」の形式で指定して認証フレームを送出する。
【０１１９】そして、認証成功後、ＩＰＣＰネゴシエーションを経て、認証フェーズを完了し、ＩＰ通信フェーズでは、割当を受けたＩＰアドレスをEthernetインタフェースに設定し、また対向アドレス(プロバイダエッジルータのＩＰアドレス)をデフォルトルートとしてルーティングテーブル（図１９にルーティングテーブルの例を示す）に設定してＩＰデータ通信をＩＰｏＥ形式で行う。
【０１２０】ただし、ネットマスクに関しては、接続したプロバイダサブネットのサブネットマスク値に従う。すなわち同一サブネットの場合は、プロバイダエッジルータを経由せずに、直接ＩＰｏＥフレームを送信する。
【０１２１】また、ＩＰ通信フェーズでは、接続性確認のフレームを定期的に送出する。認証フェーズで、ＰＰＰｏＥのネゴシエーションを行った加入者側エッジＬ２ＳＷ２０に対しては、接続セッションの維持のため、図２０に示すような接続性確認フレーム（LCP Echo-Request）を送信する。
【０１２２】そして、加入者側エッジＬ２ＳＷ２０は、LCP Echo-Requestに対して、LCP Echo-Reply を返し、ユーザが接続継続中であることを確認する。これにより、加入者側エッジＬ２ＳＷ２０が一定期間LCP Echo-Requestが受信できない場合、あるいは反対にユーザ端末装置１０がLCP Echo-Replyを一定期間受信できない場合にセッションが終了したとみなすことにより、回線断などの不慮の事態にも異常をきたすことなくセッションを終了させることができる。
【０１２３】また、接続性確認を行う場合、ユーザ端末装置１０は、プロバイダエッジルータ（ＩＰＣＰで指定を受けた対向アドレス）に対しては、Ping(ICMP Echo-Request)を送信する。これはコアＬ２ＳＷ、加入者側エッジＬ２ＳＷ２０、プロバイダ側エッジＬ２ＳＷ内の、フォワーディングテーブルのエントリにおけるエージングを回避するためである。
【０１２４】そして、ユーザ端末装置１０は、接続終了時には、接続終了を示す制御フレームを送信する。ＰＰＰであれば、図２１のような接続終了フレーム（LCP Terminate-Request）を送信する。
【０１２５】そして、加入者側エッジＬ２ＳＷ２０は、これを受けて、ユーザのＭＡＣアドレスに関するエントリをセッション管理テーブル及びＭＡＣ－ＶＩＤテーブルより削除し、LCP Terminate-Ackを返す。その後、ユーザ端末装置１０は、切断フレームであるPADTパケット(PPPoE Active Discovery Terminate、ＰＰＰｏＥ接続の終了を通知する際に使用)を送信して接続が終了する。また、このとき、ユーザ端末装置１０では、Ethernetインタフェースに設定したＩＰアドレスを削除し、ルーティングテーブルも削除する。
【０１２６】また、ユーザ端末装置１０内のユーザ側セッション管理手段１１は、一定時間ＩＰデータ通信が行われない場合に、自動的に接続を終了させることが可能な通信監視機能を持つ。ただし、実際に接続を終了するのか、あるいはどれだけの期間無通信であれば切断するのかは、ユーザが任意に設定可能とする。
【０１２７】なお、ユーザの接続先プロバイダが固定の場合などには、あらかじめユーザＩＤ(ユーザ名@プロバイダ名)及びパスワードを記憶させておき、ユーザ端末装置１０の起動時には、自動的にユーザ側セッション管理手段１１より、セッション制御を開始することにより、常時接続的な通信を行うことも可能である。
【０１２８】また、ユーザ側セッション管理手段１１は、グローバルユニークなＭＡＣアドレスが設定されたEthernetインタフェースを持つものであれば、例えば、家庭内ＬＡＮを構成している場合には、ゲートウェイルータ等に搭載されてもよい（図２２）。この場合は、上記のようにあらかじめユーザＩＤとパスワードをゲートウェイに設定しておき、家庭内ＬＡＮ側からのインターネット向けのＩＰパケットを受信したときに、ゲートウェイから自動的に発呼を行うことが可能である。
【０１２９】図２３はユーザ端末装置１０の動作を示すフローチャートである。ユーザ側セッション管理手段１１による全体動作を示している。
〔Ｓ４１〕制御フレームによるネゴシエーションを行う（認証、ＩＰアドレス割当等）。
【０１３０】〔Ｓ４２〕認証フェーズ完了か否かを判断する。完了ならばステップＳ４３へ、完了でなければステップＳ４１へ戻る。
〔Ｓ４３〕ＩＰｏＥで主信号フレームを送受信すべく、ＩＰアドレス、ルーティングテーブル等の設定を行う。

〔Ｓ４４〕ＩＰ通信の通信監視制御を行う。
【０１３１】〔Ｓ４５〕接続完了か否かを判断する。完了ならばステップＳ４７、完了でなければステップＳ４６へ行く。ここで、接続完了は、通常はユーザが明示的に行う。ただし、接続性確認フレームに対する返信が得られない場合、あるいは通信監視制御によるＩＰデータ通信の無通信検出により、接続完了処理を行うことも可能である。また、ユーザのパスワードミスなどにより、加入者側エッジＬ２ＳＷ側から接続完了処理が行われる場合もある。
【０１３２】〔Ｓ４６〕接続性確認のため、一定時間ごとに、加入者側エッジＬ２ＳＷに制御フレーム（LCP Echo Request）を、プロバイダ側エッジＬ２ＳＷにPing（ICMPEcho Request）を送信する。
〔Ｓ４７〕設定した、ＩＰアドレス及びルーティングテーブル等を削除する。
〔Ｓ４８〕接続完了を示す制御フレーム（LCP Terminate Request）を送信する。
〔Ｓ４９〕加入者側エッジＬ２ＳＷより、LCP Terminate ACKの受信後、ＰＡＤＴを送信する。ＰＡＤＴを送信して切断となる。
【０１３３】次にＡＲＰの制御に関し、最初に一般のＡＲＰ動作について説明する。ＩＰｏＥでフレームを送信する際には、通信を行う相手のＭＡＣアドレスを知る必要がある。その際には、まずARP Request を送信し、通信相手の方は、自らのＭＡＣアドレスを返信メッセージに格納して、ARP Reply(ユニキャスト)として返信する。
【０１３４】これでＩＰアドレスとＭＡＣアドレスの対応を表すARP Tableにエントリを持つ(ARPキャッシュと呼ばれ、一定期間保持される)ことになるので、ＩＰｏＥでフレームを送受信することが可能となる。
【０１３５】図２４はARP Request及びReplyのフォーマットを示す図である。ARP Request送信端末は、送信元ＭＡＣアドレスを自らのＭＡＣアドレスとし、Src Hw Addr及びSrc Prot Addrフィールドにも自らのＭＡＣアドレスとＩＰアドレスを格納して送信する。そして、知りたいのは、Tgt Prot Addrに対応するＩＰアドレスを持っている端末のTgt Hw Addr（ＭＡＣアドレス）である。
【０１３６】ARP Reply送信端末は、宛先ＭＡＣアドレスを上記のARP Request送信端末、送信元ＭＡＣアドレスを自らのＭＡＣアドレスとし、Src Hw Addr及びSrc Prot Addrに自らのＭＡＣアドレスとＩＰアドレスを格納して送信する。
【０１３７】図２５は一般のＡＲＰの動作を示す図である。ARP Requestを受信する端末、ARP Replyを受信する端末はともに、Src Hw Addr及びSrc Prot Addrフィールドからの情報をキャッシュする。すなわち、ARP Requestを受信した場合もARPエントリがキャッシュされることになる。
【０１３８】したがって、ARP Requestはブロードキャストフレームであるため、ブロードキャストドメイン内の全端末すなわち、アクセス網６経由で同一プロバイダに接続している(同一サブネットの)全ユーザに送信され、受信した端末は送信元端末のARPエントリをTableにキャッシュしてしまう。
【０１３９】この動作は企業ネットワーク等のＬＡＮセグメントでは問題ないが、プロバイダ接続ユーザは、インターネットやコンテンツなどのサービスを目的としているのであるため、プロバイダ接続ユーザ間での通信は本来の目的ではなく、ブロードキャストドメイン内の全端末にARP Requestが送信されるのは、セキュリティ的にも問題がある。
【０１４０】また、ＡＲＰをフィルタリングすると、仮にブロードキャストドメイン内のユーザ間でチャット等のP-to-P接続を行いたい、というニーズがあった場合にＭＡＣアドレスを知ることができなければ通信を行うことは不可能である。
【０１４１】また、一旦、プロバイダエッジルータに転送して、プロバイダエッジルータがあらためて相手ユーザに転送する方法も技術的には可能であるが、この場合、プロバイダエッジルータの入出力ポートが同じであり、その都度ＩＣＭＰエラーパケット(ICMP Redirect)が送出され、プロバイダエッジルータに負担がかかってしまう。すなわち、ARP Request等のブロードキャストフレームは、ブロードキャストドメイン内の全端末に送信するのではなく、本来送るべき相手にのみ送信するといった制御が必要となる。
【０１４２】次に本発明のアドレス解決手段によるＡＲＰ制御について説明する。本発明では、各加入者側エッジＬ２ＳＷは、送信元ＭＡＣアドレスでセッションを管理し、認証フェーズでユーザ端末装置１０にＩＰアドレスを割り当てるので、どのＭＡＣアドレスの端末がどのＩＰアドレスを保持しているかを表すARPエントリに相当するテーブル(図２６：以降、ARPリレーテーブルと呼ぶ)を作成することが可能である。
【０１４３】そこで本発明では、ユーザから送信されたARPフレーム(ETHER－TYPE 0x0806)について、加入者側エッジＬ２ＳＷがＭＡＣ－ＶＩＤテーブルにて認証の確認及びＶＬＡＮ－ＩＤ抽出後、ARPリレーテーブル(ＶＬＡＮ－I.D毎に持つ)を参照して、Tgt Prot Addr(ＩＰアドレス)で検索し、エントリがあれば本来のホストに代わってARP Replyを返信することを特徴とする。
【０１４４】このとき、送信元ＭＡＣアドレスは加入者側エッジＬ２ＳＷ２０のＭＡＣアドレス、Src Hw AddrとSrc Prot AddrはARPリレーテーブルでヒットしたARPエントリである。
【０１４５】もし、エントリになかった場合には、アクセス網６側に対してはタグを付加してブロードキャスト

のまま送信し、ユーザ側には送信しない(本発明の動作は、加入者側エッジＬ２ＳＷ２０のポート属性テーブルの設定で、ユーザ側ポートのブロードキャストフィルタリングを「ON」、アクセス網６側のポートを「OFF」とすることにより可能である)。

【０１４６】アクセス網６内の各エッジＬ２ＳＷ（加入者側及びｘＳＰ側）は、このタグ付きARP Request をアクセス網６側から受信し、同様に対応するＶＬＡＮ－ＩＤのARPリレーテーブルを引き、エントリを持つ加入者側エッジＬ２ＳＷがARP Replyを返す。

【０１４７】なお、本発明の動作はいわゆるProxy ARPとは異なる。Proxy ARPはルータが行う動作で、ユーザからのARP Requestに対して自身(ルータ)のＭＡＣアドレスを返し、ＩＰフレームは実際にはＬ３ルーティングにより転送する(図２７)。

【０１４８】一方、本発明の動作は、ARP Replyは本来のホストがもつエントリである。したがってＩＰフレームはレイヤ２(ＭＡＣブリッジング)で転送する。このARPリレーテーブルは、ユーザが異なるプロバイダに接続するたびに、ＩＰアドレスが変わるため、エントリも変化する。

【０１４９】したがって、このテーブルはユーザの認証フェーズ完了時に登録され、接続終了時には削除する。ただし、プロバイダエッジルータのＩＰアドレス及びＭＡＣアドレスは機器を変更したりしないかぎりは同一であるため、プロバイダエッジルータのエントリは、プロバイダ側エッジＬ２ＳＷが固定的に保持するものとする。

【０１５０】図２８は本発明のＡＲＰの制御を示す図である。ARPリレーテーブルは、通常のARP動作(ARP Request/Reply受信)でキャッシュすることはしない。したがって、あるユーザ(Ｐとする)がＩＳＰ－Ｙエッジルータの ARPエントリを知ろうとした場合には、ＩＳＰ－Ｙエッジルータが接続されたプロバイダ側エッジＬ２ＳＷがARP Reply を返し、同一プロバイダ 接続ユーザ(Ｑとする)のARPエントリを知ろうとした場合には、ユーザＱが接続された加入者側エッジＬ２ＳＷ２０がARPReplyを返すことになる。

【０１５１】存在しないエントリ対するARP Requestに対しては、どの加入者側エッジＬ２ＳＷ２０もARP Replyを返さず、アクセス網６から外に出ることなく廃棄されるので、ARP Request送信元端末のARPエントリが同一プロバイダ接続ユーザにブロードキャストされてしまうことはない。

【０１５２】また、アクセス網６内は(ＶＬＡＮ内にかぎり)ブロードキャストのまま送出するわけであるが、ＧＶＲＰやＳＴＰとの併用により、不要なポートへの送出やフレームのループ等は発生しない。

【０１５３】また本発明の動作は、プロバイダのポリシーにより、例えばプロバイダエッジルータのARPエントリ以外は返答しない(すなわちプロバイダ側エッジＬ２ＳＷ３０以外は代理でARP Replyを返さない)よう設定すれば、同一プロバイダ接続ユーザ間の通信を禁止することができ(すなわち、プロバイダ接続のみ可)、あるいはARPリレー機能をそのものをOFFにして全ユーザにARP Requestを透過させて普通のＬＡＮセグメント同様のネットワークを構成することも可能である。

【０１５４】また、ARPフレームも認証状態を確認して、ＶＬＡＮ－ＩＤの識別を行うため、各プロバイダのポリシーに応じてARPリレー機能をON/OFFしても、プロバイダ毎の仮想閉域網に閉じた接続は保持される。

【０１５５】なお、ＩＰｖ６では、ARP相当の動作は、ICMPv6で動作するNeighbor Discovery に統合された。したがってＩＰｖ６に移行した場合は、加入者側エッジＬ２ＳＷ２０内部の各ブロックでは、ＩＰｖ６フレーム(図２９)におけるNext Headerフィールドを抽出して、ICMPv6(=58)の場合にＣＰＵに回して処理を行うことになる。それ以外の場合(TCP=6 、UDP=17 など)にはそのままハードウェア処理を行う。

【０１５６】次に本発明のＡＲＰ制御に対するさらなる付加処理について説明する。上記では、加入者側エッジＬ２ＳＷ２０でARPリレーテーブルにヒットした場合、本来のユーザに代わってARP Replyを返すことを特徴とした。しかし、図２８のように端末Ｐとプロバイダエッジルータ（ＩＳＰ－Ｙエッジルータ）が通信を行う場合、端末ＰがARP Replyを受けてエントリをキャッシュし、ＩＳＰ－Ｙに対してＩＰｏＥで送信し、ＩＳＰ－Ｙエッジルータが端末Ｐに返信しようとした場合、ＩＳＰ－Ｙエッジルータには端末Ｐのエントリがキャッシュされていないため、ＩＳＰ－Ｙエッジルータも端末ＰのＭＡＣアドレスを知るためのARP Requestを送出する必要がある(ＩＰデータフレームの送受信ではARPキャッシュされない)。

【０１５７】代理応答しない本来のARPの動作であれば、ARP Requestを受信した端末は、Src Hw Addr及びSrc Prot Addrからエントリをキャッシュするため、１回のARP Request/Reply のやりとりで済む(図３０)。

【０１５８】そこで、加入者側エッジＬ２ＳＷ２０でARPリレーエントリにヒットした場合、ARP Request の送信元ＭＡＣアドレス(ブロードキャスト)を該当端末のＭＡＣアドレス(ユニキャストアドレス)に変換して該当端末にのみ転送する。

【０１５９】そのARP Requestを受け取った端末は、送信元端末に対してARP Replyを返す。このようにすれば、１回のARP Request/Replyのやりとりでお互いにARP エントリをキャッシュすることが可能となる。ここで、図３１、３２は本発明のＡＲＰ制御に関する動作シーケンスを示す図である。また、図３３、３４にＩＰ通信フェーズ及び接続性確認処理を行うシーケンス図である。

【０１６０】次に本発明のプロバイダ側エッジＬ２ＳＷ３０について説明する。プロバイダエッジルータが接続されたプロバイダ側エッジＬ２ＳＷ３０のポートは、一般にプロバイダ毎に固定である。

【０１６１】また、プロバイダエッジルータの二重化対応などで障害時にはバックアップルータに切り替わる場合なども考えられるため、プロバイダからのフレームを識別するのは、加入者側のようにＭＡＣアドレスベースではなく、ポートベースで行うことが望ましい。

【０１６２】したがって、プロバイダ側エッジＬ２ＳＷ３０では、ポートとＶＬＡＮ－ＩＤとの対応を示すポートＶＩＤテーブル(図３５)を固定的に持ち、プロバイダからのフレームは入力ポートよりプロバイダを識別し、プロバイダ毎のフォワーディングテーブル（形式は加入者側エッジＬ２ＳＷと同じ）及びポート属性テーブル(形式は加入者側エッジＬ２ＳＷと同じ)から対応するタグを付加してアクセス網６に転送し、アクセス網６側からはタグを外してプロバイダに転送する（プロバイダ側エッジＬ２ＳＷ３０に対して、ユーザ→プロバイダの制御は出力処理手段３１、プロバイダ→ユーザの制御は、送信処理手段３２で行う）。

【０１６３】なお、プロバイダ側エッジＬ２ＳＷ３０は、加入者側エッジＬ２ＳＷ２０と違い、制御フレームをハンドリングしない。なぜなら、ユーザのセッション管理は、加入者側エッジＬ２ＳＷ２０で行っており、未認証ユーザ等のアクセスも遮断しているためである。このため、不正アクセスがプロバイダに対して行われることはない。

【０１６４】また、プロバイダエッジルータ５１のARPエントリは障害等で機器そのものを交換しないかぎりは、常に一定(プロバイダエッジルータ５１のＩＰアドレスは固定でＭＡＣアドレスもEthernetインタフェースを交換しないかぎりは固定)であるため、プロバイダ側エッジＬ２ＳＷ３０は、プロバイダエッジルータ５１のARPリレーエントリを静的に持つものとする(図３５にARPリレーテーブル、その他のテーブル構成を示す)。

【０１６５】本発明のARPリレー処理では、プロバイダエッジルータ５１に対するARP Requestは、プロバイダが接続されたプロバイダ側エッジＬ２ＳＷ３０が代理でARP Replyを返す。または、プロバイダが接続されたプロバイダ側エッジＬ２ＳＷ３０がユニキャスト変換してプロバイダエッジルータ５１に転送する。

【０１６６】図３６にプロバイダ側エッジＬ２ＳＷ３０のモデル図を示す。なお、図のとおりに１台のプロバイダ側エッジＬ２ＳＷ３０ですべてのプロバイダと集中接続しなければいけないというわけではない。また、図３７にプロバイダ側エッジＬ２ＳＷ３０の機能ブロック、図３８にプロバイダ側エッジＬ２ＳＷ３０の動作を示すフローチャートを示す。

【０１６７】次に本発明の通信管理サーバ６１の認証制御手段について説明する（すなわち、Proxy Radiusサーバ６１について説明する）。本発明に関わる通信システムでは、アクセス許可(ユーザの主信号フレームを通すか通さないかの判断)、接続先プロバイダの振分け(タグを付加してアクセス網６に転送)及びシグナリング処理(ＰＰＰｏＥハンドリング)はユーザ端末装置１０が接続された加入者側エッジＬ２ＳＷ２０で行うが、ユーザの実認証はプロバイダが持っているデータベースで照合することになる。

【０１６８】このような認証に用いられるプロトコルとしてはRadius(RFC2865 ～2869)が挙げられる。RadiusはＵＤＰ（User Datagram Protocol）で動作し、ユーザＩＤやパスワードをAttribute(属性値)として扱い、Radius Access-RequestとしてRadiusクライアント(この場合、加入者側エッジＬ２ＳＷ２０側に設置)がプロバイダRadiusサーバ５２に送信して、プロバイダのデータベースで認証し、認証が成功した場合はRadius Access-Accept、失敗した場合にはRadius Access-Rejectが返される。なお、Radius Access-AcceptにはAttributeとしてユーザに割り当てるＩＰアドレス等が含まれる。

【０１６９】またRadius Accounting-Requestによってユーザの接続時間、通信データ量などをプロバイダRadiusサーバ５２に送信することによりプロバイダ側で接続に関する統計情報等を管理することができる。

【０１７０】Radiusは、ＡＤＳＬ接続等で広く用いられており、本発明でも認証プロトコルとして用いた例を上述したが、その他の認証プロトコルとしてTACACS(RFC1492)やLDAP(RFC2251)あるいはRadiusの次世代プロトコルとして標準化が進められているDiameterなど同様の機能を実現するプロトコルを利用してもよい。なお、上記の説明では、実認証をCHAPとしたが、本発明はCHAPに限るものではない（ワンタイムパスワードや指紋認証等）。

【０１７１】次にアクセス網６内に設置したProxy Radiusサーバ６１による認証フレーム転送制御方式について説明する。各加入者側エッジＬ２ＳＷ２０は、ユーザから受信したユーザＩＤ(ユーザ名@プロバイダ名)及びパスワードをRadius Access-Requestとして、認証情報を表すタグ(認証タグ)を付加してEthernetフレームでProxy Radiusサーバ６１に対して送信する。

【０１７２】一方、アクセス網６内では、認証タグを付加したフレームを認証ＶＬＡＮと識別し、ＧＶＲＰ等公知のプロトコルを用いて、Proxy Radiusサーバ６１に正しく転送されるよう設定しておく。これによりアクセス網６内のコアＬ２ＳＷ４０では、タグにもとづいて、認証情報を運ぶフレームであることを識別するので、認証情報が第三者に漏れることなくProxy Radiusサーバ６１に転送されることになる。

【０１７３】そして、Proxy Radiusサーバ６１は、プロバイダ名とＶＬＡＮ－ＩＤ及び各プロバイダRadiusサーバ５２のＩＰアドレス等の対応を示すプロバイダ管理テ

ーブルを持ち、「ユーザ名@プロバイダ名」からプロバイダを識別して、各プロバイダRadiusサーバ５２に、上記Radius Access-Request を、対応するプロバイダのタグを付加したEthernetフレームとして送信する(プロバイダ側エッジＬ２ＳＷ３０ではタグを外して転送する)。

【０１７４】プロバイダRadiusサーバ５２からはProxy Radiusサーバ６１に対してRadius Access-Accept(あるいはRejectの場合もある)が送られてくる。Proxy Radiusサーバ６１は、このRadius Access-AcceptにプロバイダのＶＬＡＮ－ＩＤを示すAttributeを追加して、加入者側エッジＬ２ＳＷ２０に転送する。加入者側エッジＬ２ＳＷ２０は認証フェーズ完了時に、Attributeで受信したＶＬＡＮ－ＩＤ値を用いてＭＡＣ－ＶＩＤテーブルに登録する。

【０１７５】したがって、加入者側エッジＬ２ＳＷ２０は、単一のProxy Radiusサーバ６１とのみ通信すればよく、また主信号フレームに付加するプロバイダのＶＬＡＮ－ＩＤもRadius Access-Acceptで示されるため、加入者側エッジＬ２ＳＷ２０でプロバイダの追加／削除に伴う登録作業を行う必要がなく(Proxy Radiusサーバ６１で一元管理すればよい)、管理工数や加入者側エッジＬ２ＳＷ２０に搭載するメモリ量が削減できる。また、プロバイダRadiusサーバ５２は、単一のRadiusクライアントとのみ通信すればよいので、プロバイダの設定に大きな変更が加わることはない（従来方式では、Ｂ－ＲＡＳが単一のRadiusクライアントとして、各プロバイダRadiusサーバと通信していた）。

【０１７６】また、加入者側エッジＬ２ＳＷ２０とProxy Radiusサーバ６１間の通信では認証タグを付加し、Proxy Radiusサーバ６１とプロバイダRadiusサーバ５２間の通信では、対応するプロバイダのタグを付加して転送するので、セキュリティも確保される。

【０１７７】図３９にProxy Radiusサーバ６１の動作を示し、Proxy Radius サーバ６１で管理するテーブルを図４０に示す。また、図４１はユーザからの認証要求から認証成功までの動作シーケンスを示す図である。

【０１７８】次に複数接続先への接続制御について説明する。従来、ＰＰＰｏＥでは、PPPoE Discovery Stageでセッション毎にユニークなＩＤ(Session－ＩＤ)が確立される。そして、PPP Session Stageでは、確立したSession－ＩＤを設定してネゴシエーション及びＩＰパケットのカプセル化転送を行う。したがって、ＰＰＰｏＥでは送信元ＭＡＣアドレスとSession－ＩＤからセッションを識別することにより、複数プロバイダに同時接続を行うことが可能である。

【０１７９】一方、本発明では、認証フェーズにおけるシグナリング処理には、ＰＰＰｏＥのメカニズムを用いるため同様に複数セッションを管理することは可能であり(図４２)、ユーザ端末装置１０に搭載したセッション管理機能においても、複数セッションを管理し、複数プロバイダに対して主信号フレームを送信することが可能である(図４３)。

【０１８０】ただし、加入者側エッジＬ２ＳＷ２０において、主信号フレームはＩＰｏＥで受信するため、Session－ＩＤフィールドが無く、送信元ＭＡＣアドレスでＭＡＣ－ＶＩＤテーブルを引くと、複数のＶＬＡＮ－ＩＤにマッチしてしまい、該当の接続先プロバイダを一意に識別することが出来ない(図４４)。

【０１８１】そこで本発明では、加入者側エッジＬ２ＳＷ２０において、送信元ＭＡＣアドレスだけでなく、複数ＶＬＡＮ－ＩＤにマッチした場合には、宛先ＭＡＣアドレスで接続先プロバイダを一意に絞るようにする。

【０１８２】宛先ＭＡＣアドレスからＶＬＡＮ－ＩＤを識別するためのテーブル(宛先ＭＡＣアドレステーブルと呼ぶ)の作成は、上述したARPリレー処理を応用する。また、上述のとおりＩＰｏＥでフレームを送信するために、相手のＭＡＣアドレスを知るため、先立ってARP Requestを送信する(ARPが解決できなければ通信できない)。

【０１８３】そして、例えば、ARPリレーテーブルにヒットしたエッジＬ２ＳＷが代理でARPReplyを返す。このARP Replyはユニキャストなので、受信したエッジＬ２ＳＷはARP ReplyのSrc Hw Addr 値とタグ(アクセス網６側からは該当プロバイダのタグを付加されて送られてくる)をもとに宛先ＭＡＣアドレステーブルに登録する。

【０１８４】このような動作により、複数同時接続時にもあらかじめARP Replyにより宛先ＭＡＣアドレステーブルが登録されているため、該当接続先を一意に識別することが可能となる。ただし、宛先ＭＡＣアドレステーブルの検索は、あくまで複数同時接続時(送信元ＭＡＣアドレスでＶＩＤテーブルを引いて複数マッチした場合)に限る。これは単一プロバイダ接続時には、送信元ＭＡＣアドレスだけで一意に識別可能であり、不要な検索を防ぐためである。また、アクセス網６側からの下りに関しては、タグより一意に識別可能であり、複数同時接続時でも動作に変更はない。

【０１８５】なお、ユーザの接続終了時は、ＰＰＰｏＥフレーム(LCP Terminate-Request、図１９)で行うため、ＭＡＣ－ＶＩＤテーブルの削除は、送信元ＭＡＣアドレスとSession－ＩＤより該当のエントリのみを削除する。本発明の動作を加えた、加入者側エッジＬ２ＳＷ２０の動作を示すフローチャート(メイン、ARPリレー処理)をそれぞれ図４５、図４６に示す。

【０１８６】次に複数接続先への同時接続時に、ユーザ端末装置１０のレイヤ２アドレスに加えて、レイヤ３アドレス（ＩＰサブネット）より、ユーザの主信号フレームの接続先を一意に識別する場合について説明する。

【０１８７】ＩＰアドレスは、ＩＰｖ４もＩＰｖ６もネットワーク部(ＩＰサブネット)とホスト部により構成さ

れ、プロバイダに接続した際、アドレスプールから割り当てられるＩＰアドレスは、ＩＰサブネットに関してはプロバイダ毎に一意であり、複数プロバイダ同時接続時、ＩＰサブネットを見ればどのプロバイダ宛てのフレームかを判断することが可能である。

【０１８８】したがって、本発明では、加入者側エッジＬ２ＳＷ２０がＩＰサブネットとＶＬＡＮ－ＩＤの対応を示すＩＰサブネットテーブルを持ち、送信元ＭＡＣアドレスでＶＬＡＮ－ＩＤを引いて複数マッチした場合、ＩＰサブネットにより該当の接続先を一意に識別することを特徴とする。

【０１８９】なお、ＩＰサブネットは、プロバイダ毎に一意で、かつ固定であるため、各エッジＬ２ＳＷはＩＰサブネットテーブルを固定的に持つものとする(図４７)。ただし、プロバイダの追加時にはProxy Radiusサーバ６１よりＳＮＭＰなどの管理プロトコルにより各エッジＬ２ＳＷに設定することも可能である。

【０１９０】なお、本発明の場合も接続先プロバイダの識別は、あくまで送信元ＭＡＣアドレスによるＶＩＤテーブルの検索が基本である(テーブルにエントリがない場合は未認証とみなして廃棄する)。

【０１９１】そして、複数マッチした場合に限り、ＩＰサブネットテーブルよりプロバイダを一意に絞る。本発明の動作を加えた、加入者側エッジＬ２ＳＷ２０の動作を示すフローチャート(メイン)を図４８に示す。

【０１９２】次に複数同時接続に対し、認証フェーズにおいて、ＩＰアドレスの割当を行うとともにアクセス網６内でプロバイダを一意に識別するタグをユーザ端末装置１０に配布して、ユーザ端末装置１０からタグを付加したかたち(IEEE802.1Qフレーム)で主信号フレームを送信する場合について説明する。

【０１９３】このような制御を行うことで、加入者側エッジＬ２ＳＷ２０では、送信元ＭＡＣアドレスによるＭＡＣ－ＶＩＤテーブルの検索で複数マッチした場合(エントリがない場合は廃棄)に、タグを見て一意に絞ることが可能となる。

【０１９４】なお、タグを見ただけで接続先を一意に判別することは可能であるが、正しく認証されているかは判断できない(不正にタグを付加して送信してきたのかもしれない)ので、送信元ＭＡＣアドレスでＭＡＣ－ＶＩＤテーブルのチェックは必須である。あるいは、タグから接続先プロバイダを一意に識別後、ＭＡＣ－ＶＩＤテーブルに該当のエントリがあるかチェックする方法でも構わない。

【０１９５】この場合、加入者側エッジＬ２ＳＷ２０のポート属性テーブル（図１０）の設定としては、ユーザ側ポートでもIEEE802.1Qフレームを受信可能にし、タグ挿抜を「With Tag」に設定することで対応することができる。

【０１９６】なお、プロバイダ側エッジＬ２ＳＷ３０では、これまでと同様にタグを外してプロバイダエッジルータ５１に転送する。そしてプロバイダ側からのフレームは入力ポートから対応するタグを識別／付加してアクセス網６を転送する(図５０)。これらの動作を加えた加入者側エッジＬ２ＳＷ２０の動作を示すフローチャート(メイン)を図４９に示す。

【０１９７】なお、ＰＰＰｏＥでカプセル化する場合と異なり、IEEE802.3ac-1998準拠のEthernetインタフェースカードであれば、ユーザ端末装置１０でIEEE802.1Q ＶＬＡＮ－Ｔａｇを付加した場合でもＭＴＵが１５００バイトのＩＰパケットの送受信が可能である。

【０１９８】次に本発明の通信管理サーバのセッション管理手段について説明する（以降の説明ではセッション管理サーバと呼ぶ）。加入者側エッジＬ２ＳＷ２０では、ETHER－TYPEでフレームを判別し、主信号フレームはアクセス許可(ユーザの主信号フレームを通すか通さないかの判断)及び接続先プロバイダの振分け(タグを付加してアクセス網６に転送)をハードウェア処理、制御フレームによるシグナリング処理(ＰＰＰｏＥハンドリング)をソフトウェア処理で行うことを特徴としたが、ここでは、シグナリング処理に関しては、アクセス網６内に設置したセッション管理サーバで集中的に行い、主信号フレーム処理と制御フレーム処理を装置的に分離処理する場合について説明する。

【０１９９】上述したように、ＰＰＰにおける制御情報のネゴシエーションは、ユーザ毎に条件も異なるため処理負荷が大きい。本発明ではユーザ端末装置１０が接続された加入者側エッジＬ２ＳＷ２０にて分散処理しているため、Ｂ－ＲＡＳに比べると負荷は小さいものの、加入者側エッジＬ２ＳＷ２０の負荷は小さいほうが望ましい。

【０２００】そこで、加入者側エッジＬ２ＳＷ２０にて制御フレームをハンドリングするのではなく、主信号フレーム同様にハードウェア処理でアクセス網６内に設置したセッション管理サーバに転送する。

【０２０１】セッション管理サーバは上述の図７で示したセッション管理テーブルを持ち、ユーザとネゴシエーションを行う。ただし、アクセス許可及び主信号フレームの接続先プロバイダへの振分けは、加入者側エッジＬ２ＳＷ２０で行うため、認証フェーズ完了後、セッション管理サーバからユーザが接続された加入者側エッジＬ２ＳＷ２０を設定(ＭＡＣ－ＶＩＤテーブルの遠隔設定)する必要がある。

【０２０２】設定自体はＳＮＭＰなど既存の管理プロトコルで可能であるが、加入者側エッジＬ２ＳＷ２０を経由して転送されてきたユーザの制御フレームには、加入者側エッジＬ２ＳＷ２０を識別する情報が含まれていないため、どのエッジＬ２ＳＷ配下にユーザが接続されているか判断できない。

【０２０３】そこで、制御フレームに関しては、加入者

側エッジＬ２ＳＷ２０を識別するタグを付加してセッション管理サーバに転送する。すなわち、主信号フレームに付加するタグは、プロバイダを識別するものであったが、制御フレームに付加するタグは加入者側エッジＬ２ＳＷ２０自身を識別するものとなる。ただし、加入者側エッジＬ２ＳＷ２０の動作としては、テーブルからタグを引いて付加するにすぎない。なお、ETHER-TYPEが制御フレーム（例えば、0x8863）であれば、このタグを付加するというテーブル（付加するタグは、セッション管理サーバが加入者側エッジＬ２ＳＷを識別できるＩＤ値）を持っていることになる。

【０２０４】そして、セッション管理サーバでは、受信フレームの送信元ＭＡＣアドレス(ユーザ端末装置１０のＭＡＣアドレス)でユーザのセッションを管理し、タグでどの加入者側エッジＬ２ＳＷ２０配下であるかを把握することができる。なお、プロバイダRadiusサーバ５２との通信はこの場合、セッション管理サーバがRadiusクライアントとして直接プロバイダRadiusサーバ５２と行うことになる。

【０２０５】これはプロバイダ から見て単一のRadiusクライアントと通信することに変わりはない。図５１及び図５２にセッション管理サーバの動作による接続イメージを示す。図５２に示すように主信号フレームの流れについては変更はない。

【０２０６】また、図５３に加入者側エッジＬ２ＳＷの機能ブロック図を示す。図５４は動作シーケンスを示す図である。なお、ユーザ端末装置１０に搭載する機能や、プロバイダ側エッジＬ２ＳＷ５１及びプロバイダ側の他装置に関しても変更はない。

【０２０７】以上説明したように、本発明により、加入者側エッジＬ２ＳＷ２０は、主信号フレームも制御フレームもハード的に転送するだけなので、処理負荷が大幅に軽減される。またセッション管理は一箇所に集中することになるが、専用機器(サーバ)で処理するため、処理増大にともなうＣＰＵやメモリのアップグレードは容易である。あるいは分散装置等を用いてセッション管理を複数サーバに分散させることも可能である。

【０２０８】次にセッション管理サーバの他の制御について説明する。セッション管理サーバは、ユーザ認証完了後にARPリレーテーブルを作成し、ユーザ端末装置１０から送信されたARP Requestは加入者側エッジＬ２ＳＷ にてタグを付加してセッション管理サーバに転送する（ETHER TYPE=0x0806からＡＲＰであることを判別して、ハードウェア処理でタグを付加して転送する）。このタグはARPフレームを識別するタグをアクセス網６内で規定したものを用いる。

【０２０９】アクセス網６内では、このタグが付加されたフレームは、ＧＶＲＰ等公知の管理プロトコルにより、宛先不明の場合すなわちARP Request(ブロードキャスト)が不用意なフラッディングが行われること無く、セッション管理サーバに転送されるよう設定しておく。

【０２１０】そして、セッション管理サーバは、ARP Requestを受信し、ARPリレーテーブルにヒットした場合は、送信元ユーザに代理でARP Reply を返したり、または、ブロードキャストをユニキャストに変換して該当端末にのみ転送する。これによりユーザの秘匿性を確保しつつ、ＩＰｏＥでの通信が可能となる。図５５はセッション管理サーバの動作を示す図であり、図５６、５７は動作シーケンスを示す図である。

【０２１１】次に従来方式による接続先切り替え通信も収容する場合について説明する。ユーザ端末装置１０が接続された加入者側エッジＬ２ＳＷ２０において、ＰＰＰｏＥフレーム(ETHER－TYPE 0x8864)をＣＰＵに回して処理する際に、ＰＰＰ－PROTOCOL値が0x0021すなわちＩＰパケットをカプセル化したフレームであった場合には、ＭＡＣ－ＶＩＤテーブルを参照して、接続先プロバイダのタグを抽出し(エントリにない場合は廃棄)、デカプセル化して、かつタグを付加したＩＰｏＥフレームとしてアクセス網６に転送する。

【０２１２】アクセス網６内のコアＬ２ＳＷ４０及びプロバイダ側エッジＬ２ＳＷ３０の動作及び他のプロバイダ側設備に変更は必要ない。そしてプロバイダからの下りフレームは、加入者側エッジＬ２ＳＷ２０において、再びカプセル化を行ってユーザに転送する。

【０２１３】なお、本発明の動作は実際にはＢ－ＲＡＳ同等の仮想ルータ機能を行うものである。すなわち、ユーザ端末装置１０から受信したＩＰ over ＰＰＰ over Ethernet フレームをデカプセル化してアクセス網６に転送する際に、送信元ＭＡＣアドレスは自Ｌ２ＳＷのＭＡＣアドレス、宛先ＭＡＣアドレスをプロバイダエッジルータのＭＡＣアドレスに付け替え、下りフレーム(宛先ＭＡＣアドレスが自Ｌ２ＳＷ宛て)はＣＰＵに回して転送先ユーザを決定し、宛先ＭＡＣアドレスを該当ユーザ端末装置１０のＭＡＣアドレス、送信元ＭＡＣアドレスを自Ｌ２ＳＷのＭＡＣアドレスに付け替えて転送する。

【０２１４】このような動作はソフトウェア処理が前提となるが、あくまで本発明の通信システム１において従来方式を収容するための手段であり、本発明のユーザ端末装置１０と通信を行う場合は、主信号フレームはハードウェアによる高速処理を行うことに変わりはない。また上記のような動作をソフトウェア処理により行うことで、従来技術の内容を付加機能として組み込むことは容易である。

【０２１５】図５８は本発明の動作を付加した場合の接続イメージ(ユーザ端末装置からＩＰ over ＰＰＰ over Ethernetで送出された場合)を示す。また、図５９に本発明の方式と従来方式の場合の加入者側エッジＬ２ＳＷ内部でのＩＰデータの流れを示す。

【０２１６】次に本発明の通信接続プログラムについて

説明する。本発明であるユーザ端末装置１０の処理機能は、通信接続プログラムとして、クライアントコンピュータによって実現することができる。その場合、本発明のクライアントに相当する装置が有すべき機能の処理内容を記述したクライアントプログラムが提供される。

【０２１７】そして、上記のようなコンピュータプログラムは、半導体メモリや磁気記録媒体などの記録媒体に記述させることができる。これにより、市場に流通させる場合に、ＣＤ－ＲＯＭやフレキシブルディスク等の可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。また、コンピュータで実行する際には、コンピュータ内のハードディスク装置等にプログラムを格納しておき、メインメモリにロードして実行する。

【０２１８】次に本発明の通信システム１の変形例として、加入者側／コア（アクセス網）側／ｘＳＰ側が一体となったＬ２ＳＷを用いた場合のシステムについて説明する。

【０２１９】図６０は一体型のＬ２ＳＷを含む通信システムを示す図である。通信システム１ａは、ユーザ端末装置１０、通信管理サーバ６１、加入者側／コア（アクセス網）側／ｘＳＰ側が一体となったＬ２ＳＷ７０、ｘＳＰから構成される。

【０２２０】一体型のスイッチを実現するためには、各ポートの属性を明確化し、加入者側ポートならば（送信元）ＭＡＣアドレスからＭＡＣ－ＶＩＤテーブルを引き、コア（アクセス網）側であれば、タグからＶＩＤを認識し、ｘＳＰ側であれば入力ポートからポートＶＩＤテーブルを引くという動作が必要となる。

【０２２１】そこで、上述のポート属性テーブルＴ２ｄに変更を加え（図６１に加入者側のポート属性テーブル、図６２にｘＳＰ側のポート属性テーブルを示す）、テーブルにポート属性というパラメータを追加し、その設定によって、そのポートが加入者側なのかｘＳＰ側なのかコア（アクセス網）側なのかを設定するようにする。

【０２２２】例えば、コマンドラインで、#configure port 1 user、#configure port 5coreなどと設定すると、各ポートがそれぞれの側に対応した設定になるようにする（ＶＩＤフィールドに関しては後述）。

【０２２３】そして、その他のパラメータ、すなわち受信フレーム（入力時に受け入れるフレーム）、ブロードキャストフィルタリング（ブロードキャストフレームやフラッディング時にそのポートより出力するかフィルタリングするか）及びタグ挿抜（タグを付けて出力するか）は、ポート属性値よりデフォルト値（例えば、加入者側であれば、受信フレームは「PPPoE、IP、ARP」、ブロードキャストフィルタリングは「ＯＮ」、タグ挿抜は「ＵｎＴａｇ」）が自動的に設定されるように変更する（つまり、ポート属性テーブルで、受信フレーム／ブロードキャストフィルタリング／タグ挿抜のそれぞれの値を逐一設定することを回避する）。

【０２２４】また、ｘＳＰ側のＬ２ＳＷのポート属性テーブルの設定値には、（ＶＩＤを静的に設定するため）ＶＩＤ値も同時に設定する。例えば、configure port 7 xspvid 12と設定すると、ポート７をｘＳＰ側設定とし、ＶＩＤが１２となる。

【０２２５】一方、図１の送信処理手段で参照されるポートＶＩＤテーブルは、本ユーザ設定値より登録され、主信号フレームはポートＶＩＤテーブルにより、ＶＩＤが識別され、ＶＩＤごとのフォワーディングテーブル（アドレス学習により自動生成）により転送される。コア側及びユーザ側のＶＩＤは不定な（接続先毎に変わる）ので設定はしない。

【０２２６】そして、加入者側とｘＳＰ側が一体となったＬ２ＳＷでは、フレーム入力時にポート属性テーブルから受信可能なETHER TYPEをチェックするとともに、ポート属性テーブルから主信号フレームのＶＩＤを判断する。以降フォワーディング、出力処理は変わらない。なお、図６３に一体型のＬ２ＳＷのブロック図を、図６４に動作フローチャートを示す。

【０２２７】（付記１）　ユーザからは、ＩＰｏＥで主信号フレームを送受信し、前記ユーザでは、レイヤ２レベルで前記主信号フレームと区別可能な制御フレームによって、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、アクセス網にとっては、接続先仮想閉域網を識別して、送信元ＭＡＣアドレスと、前記接続先仮想閉域網とをマッピングし、前記アクセス網では、ＭＡＣブリッジングによってレイヤ２レベルの転送を行うことを特徴とする通信方法。

【０２２８】（付記２）　アクセス網と、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、から構成されて仮想閉域網に対するレイヤ２での接続を行うユーザ端末装置と、を有することを特徴とする通信システム。

【０２２９】（付記３）　前記ユーザ側セッション管理手段は、通信フェーズ時に、接続性確認フレームを定期的に送信することを特徴とする付記２記載の通信システム。

（付記４）　前記ユーザ側セッション管理手段は、主信号フレームの送受信を監視し、ユーザ設定可能な一定時間に、主信号フレームの通信が行われない場合は、自動的に接続を終了させることを特徴とする付記２記載の通信システム。

【０２３０】（付記５）　前記制御フレームの受信時に

は、シグナリング制御を行う網側セッション管理手段と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、前記接続先から転送された主信号フレームの受信時には、前記タグを外して前記ユーザ端末装置側へ転送する転送制御手段と、から構成される加入者側エッジスイッチ装置をさらに有することを特徴とする付記２記載の通信システム。

【０２３１】（付記６）　前記網側セッション管理手段は、前記レイヤ２アドレスとユーザとのセッション対応を示すテーブルを用いて、ソフトウェア処理でシグナリング制御を行い、前記転送制御手段は、前記レイヤ２アドレスと前記接続先毎の前記タグとの対応を示すテーブルと、前記接続先毎に独立したフォワーディング情報を示すテーブルと、各ポートの属性を示すテーブルとを用いて、ハードウェア処理で、主信号フレームの転送を行うことを特徴とする付記５記載の通信システム。

【０２３２】（付記７）　前記転送制御手段は、各ポートの属性を示す前記テーブルにもとづいて、入力フレームの受け入れ可否の判断、出力フレームのタグ挿抜またはブロードキャストフィルタリングのＯＮ／ＯＦＦの判断、ユニキャストのフラッディングのフィルタリング処理を行うことを特徴とする付記５記載の通信システム。

【０２３３】（付記８）　前記転送制御手段は、カプセル化された主信号を受信した場合には、デカプセル化した後に、前記タグを付加して転送することを特徴とする付記５記載の通信システム。

【０２３４】（付記９）　複数の前記接続先と同時接続する場合、前記転送制御手段は、前記ユーザ端末装置及び前記接続先それぞれのレイヤ２アドレスにより、接続先を一意に識別することを特徴とする付記５記載の通信システム。

【０２３５】（付記１０）　複数の前記接続先と同時接続する場合、前記転送制御手段は、前記ユーザ端末装置のレイヤ２アドレス及び前記接続先のレイヤ３アドレスにより、接続先を一意に識別することを特徴とする付記５記載の通信システム。

【０２３６】（付記１１）　前記網側セッション管理手段は、シグナリング制御時に前記タグを前記ユーザ端末装置へ配布し、複数の前記接続先と同時接続する場合、前記主信号送受信手段は、前記タグを付加した主信号フレームを前記加入者側エッジスイッチ装置に送信して、前記加入者側エッジスイッチ装置が接続先を一意に識別することを特徴とする付記５記載の通信システム。

【０２３７】（付記１２）　前記タグと出力ポートとが対応して、前記タグを外して前記接続先へ主信号フレームを出力する出力処理手段と、入力ポートより前記接続先を判断し、前記タグを付加して前記ユーザ端末装置側へ送信する送信処理手段と、から構成される接続先側エッジスイッチ装置をさらに有することを特徴とする付記２記載の通信システム。

【０２３８】（付記１３）　前記加入者側エッジスイッチ装置及び前記接続先側エッジスイッチ装置は、レイヤ２アドレスとレイヤ３アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ２アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ２アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする付記２記載の通信システム。

【０２３９】（付記１４）　前記アドレス解決手段は、前記送信元装置のレイヤ２アドレスを前記宛先装置へユニキャスト転送することを特徴とする付記１３記載の通信システム。

【０２４０】（付記１５）　前記ユーザ端末装置からの認証情報の集約、前記認証情報の前記接続先への転送、前記接続先で認証制御された結果を示す認証メッセージの前記ユーザ端末装置への転送、を含む認証に関する一元管理処理を行う通信管理サーバをさらに有することを特徴とする付記２記載の通信システム。

【０２４１】（付記１６）　前記網側セッション管理手段を前記通信管理サーバに、前記転送制御手段を前記加入者側エッジスイッチ装置に持たせて、前記制御フレームの処理と、前記主信号フレームの処理とを装置的に分離することを特徴とする付記１５記載の通信システム。

【０２４２】（付記１７）　前記加入者側エッジスイッチ装置は、前記ユーザ端末装置からの前記制御フレームに、自配下にユーザが存在することを示すタグを付加して、ハードウェア処理で前記通信管理サーバに送信し、前記通信管理サーバでは、認証成功時に、前記加入者側エッジスイッチ装置に、接続先を識別するためのテーブルを遠隔設定することを特徴とする付記１５記載の通信システム。

【０２４３】（付記１８）　前記通信管理サーバは、レイヤ２アドレスとレイヤ３アドレスの対応を示すテーブルを生成し、前記加入者側エッジスイッチ装置は、宛先装置のレイヤ２アドレスを求めるリクエストを、ハードウェア処理で前記通信管理サーバに送信して、アドレス解決制御を行うことを特徴とする付記１５記載の通信システム。

【０２４４】（付記１９）　認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行うユーザ側セッション管理手段と、通信フェーズ時に、カプセル化しない主信号フレームを送受信する主信号送受信手段と、を有することを特徴とする、仮想閉域網に対するレイヤ２での接続を行うユーザ端末装置。

【０２４５】（付記２０）　前記ユーザ側セッション管理手段は、通信フェーズ時に、接続性確認フレームを定期的に送信することを特徴とする付記１９記載のユーザ

端末装置。
【０２４６】（付記２１）　前記ユーザ側セッション管理手段は、主信号フレームの送受信を監視し、ユーザ設定可能な一定時間に、主信号フレームの通信が行われない場合は、自動的に接続を終了させることを特徴とする付記１９記載のユーザ端末装置。
【０２４７】（付記２２）　複数の前記接続先と同時接続する場合、前記主信号送受信手段は、ネットワーク側から配布された接続先を一意に示すタグを付加した主信号フレームを送信することを特徴とする付記１９記載のユーザ端末装置。
【０２４８】（付記２３）　制御フレームの受信時には、シグナリング制御を行う網側セッション管理手段と、ユーザから転送された主信号フレームの受信時には、仮想閉域網を一意に示すタグを付加して転送し、接続先から転送された主信号フレームの受信時には、前記タグを外してユーザ端末装置側へ転送する転送制御手段と、を有することを特徴とする加入者側エッジスイッチ装置。
【０２４９】（付記２４）　前記網側セッション管理手段は、前記レイヤ２アドレスとユーザとのセッション対応を示すテーブルを用いて、ソフトウェア処理でシグナリング制御を行い、前記転送制御手段は、前記レイヤ２アドレスと前記接続先毎の前記タグとの対応を示すテーブルと、前記接続先毎に独立したフォワーディング情報を示すテーブルと、各ポートの属性を示すテーブルとを用いて、ハードウェア処理で、主信号フレームの転送を行うことを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５０】（付記２５）　前記転送制御手段は、各ポートの属性を示す前記テーブルにもとづいて、入力フレームの受け入れ可否の判断、出力フレームのタグ挿抜またはブロードキャストフィルタリングのＯＮ／ＯＦＦの判断、ユニキャストのフラッディングのフィルタリング処理を行うことを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５１】（付記２６）　レイヤ２アドレスとレイヤ３アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ２アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ２アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５２】（付記２７）　前記アドレス解決手段は、前記送信元装置のレイヤ２アドレスを前記宛先装置へユニキャスト転送することを特徴とする付記２６記載の加入者側エッジスイッチ装置。
【０２５３】（付記２８）　複数の前記接続先と同時接続する場合、前記転送制御手段は、ユーザ端末装置及び前記接続先それぞれのレイヤ２アドレスにより、接続先を一意に識別することを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５４】（付記２９）　複数の前記接続先と同時接続する場合、前記転送制御手段は、ユーザ端末装置のレイヤ２アドレス及び前記接続先のレイヤ３アドレスにより、接続先を一意に識別することを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５５】（付記３０）　前記網側セッション管理手段は、ユーザが複数の前記接続先と同時接続する際には、シグナリング制御時に前記タグを前記ユーザ端末装置へ配布することを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５６】（付記３１）　前記転送制御手段は、カプセル化された主信号を受信した場合には、デカプセル化した後に、前記タグを付加して転送することを特徴とする付記２３記載の加入者側エッジスイッチ装置。
【０２５７】（付記３２）　タグと出力ポートとが対応して、前記タグを外して接続先へ主信号フレームを出力する出力処理手段と、入力ポートより前記接続先を判断し、前記タグを付加してユーザ端末装置側へ送信する送信処理手段と、を有することを特徴とする接続先側エッジスイッチ装置。
【０２５８】（付記３３）　レイヤ２アドレスとレイヤ３アドレスの対応を示すテーブルを生成し、送信元装置から宛先装置のレイヤ２アドレスを求めるリクエストがあった場合、前記テーブルにもとづき、前記宛先装置の代理応答を行って、前記レイヤ２アドレスを返信して、アドレス解決制御を行うアドレス解決手段をさらに有することを特徴とする付記３２記載の接続先側エッジスイッチ装置。
【０２５９】（付記３４）　前記アドレス解決手段は、前記送信元装置のレイヤ２アドレスを前記宛先装置へユニキャスト転送することを特徴とする付記３３記載の接続先側エッジスイッチ装置。
【０２６０】（付記３５）　接続先を一意に示すタグを参照するタグ参照手段と、レイヤ２で主信号フレームの転送を行うコアスイッチング転送手段と、を有することを特徴とするコアスイッチ装置。
【０２６１】（付記３６）　認証サーバとして動作する際、ユーザ端末装置からの認証情報の集約、前記認証情報の接続先への転送、前記接続先で認証制御された結果を示す認証メッセージの前記ユーザ端末装置への転送、を含む認証に関する一元管理処理を行う認証制御手段と、セッション管理サーバとして動作する際、制御フレームの受信時に、シグナリング制御を行うセッション管理手段と、を有することを特徴とする通信管理サーバ。
【０２６２】（付記３７）　前記認証制御手段と前記ユーザ端末装置間で、認証タグが付加された認証情報により、前記認証情報を含むフレームであることを認識して

通信を行うことを特徴とする付記３６記載の通信管理サーバ。

【０２６３】（付記３８）　前記セッション管理手段は、加入者側エッジスイッチ装置から送信された、自配下にユーザが存在することを示すタグが付加された制御フレームを受信し、認証成功時には、前記加入者側エッジスイッチ装置に、接続先を識別するためのテーブルを遠隔設定することを特徴とする付記３６記載の通信管理サーバ。

【０２６４】（付記３９）　前記セッション管理手段は、レイヤ２アドレスとレイヤ３アドレスの対応を示すテーブルを生成し、前記加入者側エッジスイッチ装置は、宛先装置のレイヤ２アドレスを求めるリクエストを、ハードウェア処理で前記通信管理サーバに送信して、アドレス解決制御を行うことを特徴とする付記３６記載の通信管理サーバ。

【０２６５】（付記４０）　ユーザ端末装置側に装備され、仮想閉域網に対するレイヤ２での接続を行う通信接続プログラムにおいて、コンピュータに、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、通信フェーズ時に、カプセル化しない主信号フレームを送受信する、処理を実行させることを特徴とする通信接続プログラム。

【０２６６】（付記４１）　通信フェーズ時に、接続性確認フレームを定期的に送信する処理をさらに含むことを特徴とする付記４０記載の通信接続プログラム。（付記４２）　主信号フレームの送受信を監視し、ユーザ設定可能な一定時間に、主信号フレームの通信が行われない場合は、自動的に接続を終了させる処理をさらに含むことを特徴とする付記４０記載の通信接続プログラム。

【０２６７】（付記４３）　複数の前記接続先と同時接続する場合、ネットワーク側から配布された接続先を一意に示すタグを付加した主信号フレームを送信する処理をさらに含むことを特徴とする付記４０記載の通信接続プログラム。

【０２６８】

【発明の効果】以上説明したように、本発明の通信方法は、ユーザからは、ＩＰｏＥでの主信号フレームの送受信及び制御フレームによって、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、アクセス網にとっては、接続先仮想閉域網を識別して、送信元ＭＡＣアドレスと、接続先仮想閉域網とをマッピングして、ＭＡＣブリッジングによってレイヤ２レベルの転送を行うこととした。これにより、レイヤ２レベルでの高速通信可能なＶＰＮシステムを構築することができるので、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【０２６９】また、本発明の通信システムは、レイヤ２での通信接続を行うユーザ端末装置で、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、通信フェーズ時には、カプセル化しない主信号フレームを送受信する処理を行い、また、ユーザ側／接続側のエッジスイッチ装置では、主信号フレームに対してタグの挿抜を行って、レイヤ２レベルでの転送を行う構成とした。これにより、レイヤ２レベルでの高速通信可能なＶＰＮシステムを構築することができるので、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【０２７０】さらに、本発明のユーザ端末装置は、認証フェーズ時に、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、通信フェーズ時には、カプセル化しない主信号フレームを送受信する処理を行う構成とした。これにより、レイヤ２レベルでの高速通信可能なＶＰＮシステムに対して、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【０２７１】また、本発明の通信接続プログラムは、制御フレームを用いて、接続先の指定、ユーザ認証及びＩＰアドレス割り当ての処理を含む制御を行い、通信フェーズ時には、カプセル化しない主信号フレームを送受信する処理を行うこととした。これにより、レイヤ２レベルでの高速通信可能なＶＰＮシステムに対して、ユーザは接続先を任意に切り替えて、効率よくサービスを受けることができ、ユーザとプロバイダ間での通信サービスの品質及び利便性の向上を図ることが可能になる。

【図面の簡単な説明】

【図１】本発明の通信システムの原理図である。

【図２】フレーム構成を示す図である。（Ａ）は改正前、（Ｂ）は改正後、（Ｃ）はＰＰＰｏＥでカプセル化した場合のフレーム構成を示している。

【図３】通信システムの構成例を示す図である。

【図４】主信号フレームのフォーマットを示す図である。

【図５】主信号フレームのフォーマットを示す図である。

【図６】認証フェーズ時のシーケンスを示す図である。

【図７】加入者側エッジＬ２ＳＷが有するテーブルを示す図である。

【図８】加入者側エッジＬ２ＳＷが有するテーブルを示す図である。

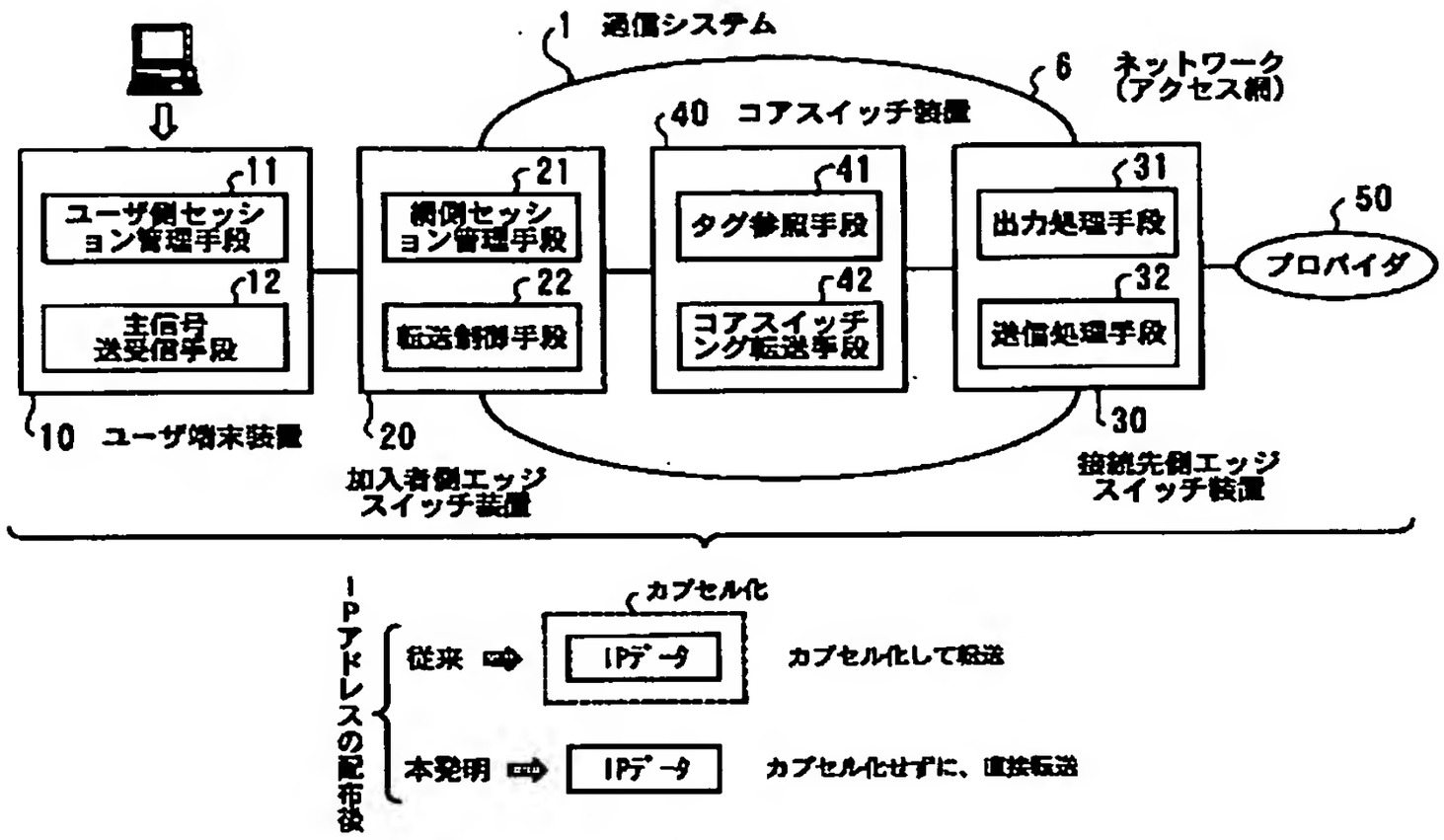
【図９】加入者側エッジＬ２ＳＷが有するテーブルを示す図である。

【図１０】加入者側エッジＬ２ＳＷが有するテーブルを

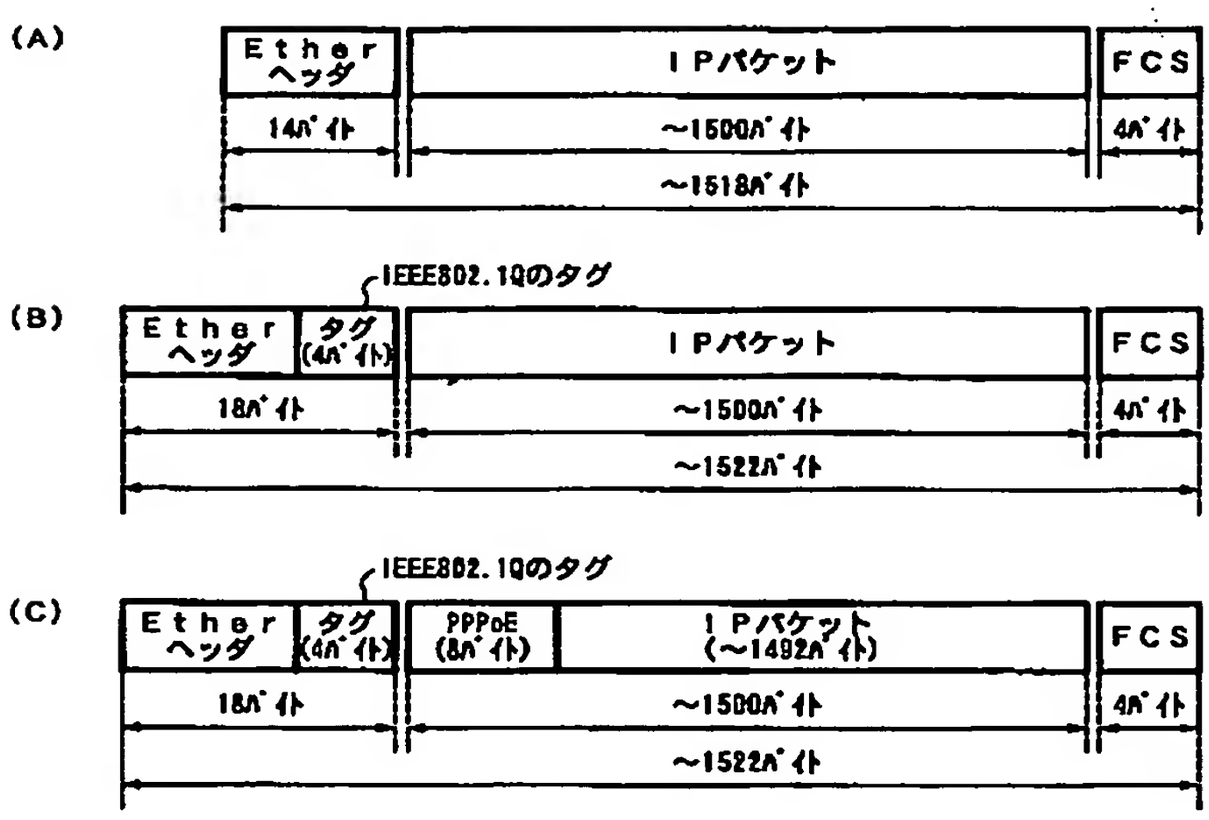
示す図である。
【図１１】加入者側エッジＬ２ＳＷの動作概要を示す図である。
【図１２】加入者側エッジＬ２ＳＷのブロック構成を示す図である。
【図１３】加入者側エッジＬ２ＳＷの全体動作を示すフローチャートである。
【図１４】加入者側エッジＬ２ＳＷのＰＰＰｏＥネゴシエーションの動作を示すフローチャートである。
【図１５】加入者側エッジＬ２ＳＷのフォワーディング処理／出力処理の動作を示すフローチャートである。
【図１６】ユーザ端末装置の構成を示す図である。
【図１７】従来のユーザ端末におけるプロトコルスタックを示す図である。
【図１８】ユーザ側セッション管理テーブルを示す図である。
【図１９】ルーティングテーブルを示す図である。
【図２０】LCP Echo-Requestのフォーマット構成を示す図である。
【図２１】LCP Terminate-Requestのフォーマット構成を示す図である。
【図２２】ゲートウェイルータを用いたシステム例を示す図である。
【図２３】ユーザ端末装置の動作を示すフローチャートである。
【図２４】ARP Request及びReplyのフォーマットを示す図である。
【図２５】一般のＡＲＰの動作を示す図である。
【図２６】ＡＲＰリレーテーブルを示す図である。
【図２７】Proxy ARPの動作を示す図である。
【図２８】本発明のＡＲＰの制御を示す図である。
【図２９】ＩＰｖ６データフレームのフォーマットを示す図である。
【図３０】本発明のＡＲＰの制御を示す図である。
【図３１】動作シーケンスを示す図である。
【図３２】動作シーケンスを示す図である。
【図３３】ＩＰ通信フェーズ及び接続性確認処理を行うシーケンス図である。
【図３４】ＩＰ通信フェーズ及び接続性確認処理を行うシーケンス図である。
【図３５】プロバイダ側エッジＬ２ＳＷが有するテーブルを示す図である。
【図３６】プロバイダ側エッジＬ２ＳＷのモデル図である。
【図３７】プロバイダ側エッジＬ２ＳＷのブロック構成を示す図である。
【図３８】プロバイダ側エッジＬ２ＳＷの動作を示すフローチャートである。
【図３９】Proxy Radiusサーバの動作を説明する図である。
【図４０】プロバイダ管理テーブルを示す図である。
【図４１】動作シーケンスを示す図である。
【図４２】複数同時接続時のセッション管理テーブルを示す図である。
【図４３】複数同時接続のイメージ図である。
【図４４】宛先ＭＡＣアドレステーブルを示す図である。
【図４５】複数マッチした場合の加入者側エッジＬ２ＳＷの動作を示すフローチャートである。
【図４６】複数マッチした場合のＡＲＰリレー処理を示すフローチャートである。
【図４７】ＩＰサブネットテーブルを示す図である。
【図４８】複数マッチした場合の加入者側エッジＬ２ＳＷの動作を示すフローチャートである。
【図４９】加入者側エッジＬ２ＳＷの動作を示すフローチャートである。
【図５０】接続イメージを示す図である。
【図５１】接続イメージを示す図である。
【図５２】接続イメージを示す図である。
【図５３】加入者側エッジＬ２ＳＷのブロック構成を示す図である。
【図５４】動作シーケンスを示す図である。
【図５５】セッション管理サーバの動作を示す図である。
【図５６】動作シーケンスを示す図である。
【図５７】動作シーケンスを示す図である。
【図５８】接続イメージを示す図である。
【図５９】加入者側エッジＬ２ＳＷのＩＰデータの流れを示す図である。
【図６０】一体型のＬ２ＳＷを含む通信システムを示す図である。
【図６１】加入者側のポート属性テーブルを示す図である。
【図６２】ｘＳＰ側のポート属性テーブルを示す図である。
【図６３】一体型のＬ２ＳＷのブロック図である。
【図６４】動作フローチャートを示す図である。
【図６５】ユーザとプロバイダとの接続形態を示す図である。
【図６６】ＰＰＰｏＥを利用した従来のネットワークシステムを示す図である。
【符号の説明】
１　通信システム
１０　ユーザ端末装置
１１　ユーザ側セッション管理手段
１２　主信号送受信手段
２０　加入者側エッジスイッチ装置
２１　網側セッション管理手段
２２　転送制御手段
３０　接続先側エッジスイッチ装置

31　出力処理手段
32　送信処理手段
40　コアスイッチ装置
41　タグ参照手段
42　コアスイッチング転送手段
50　プロバイダ
6　アクセス網

【図1】




【図2】

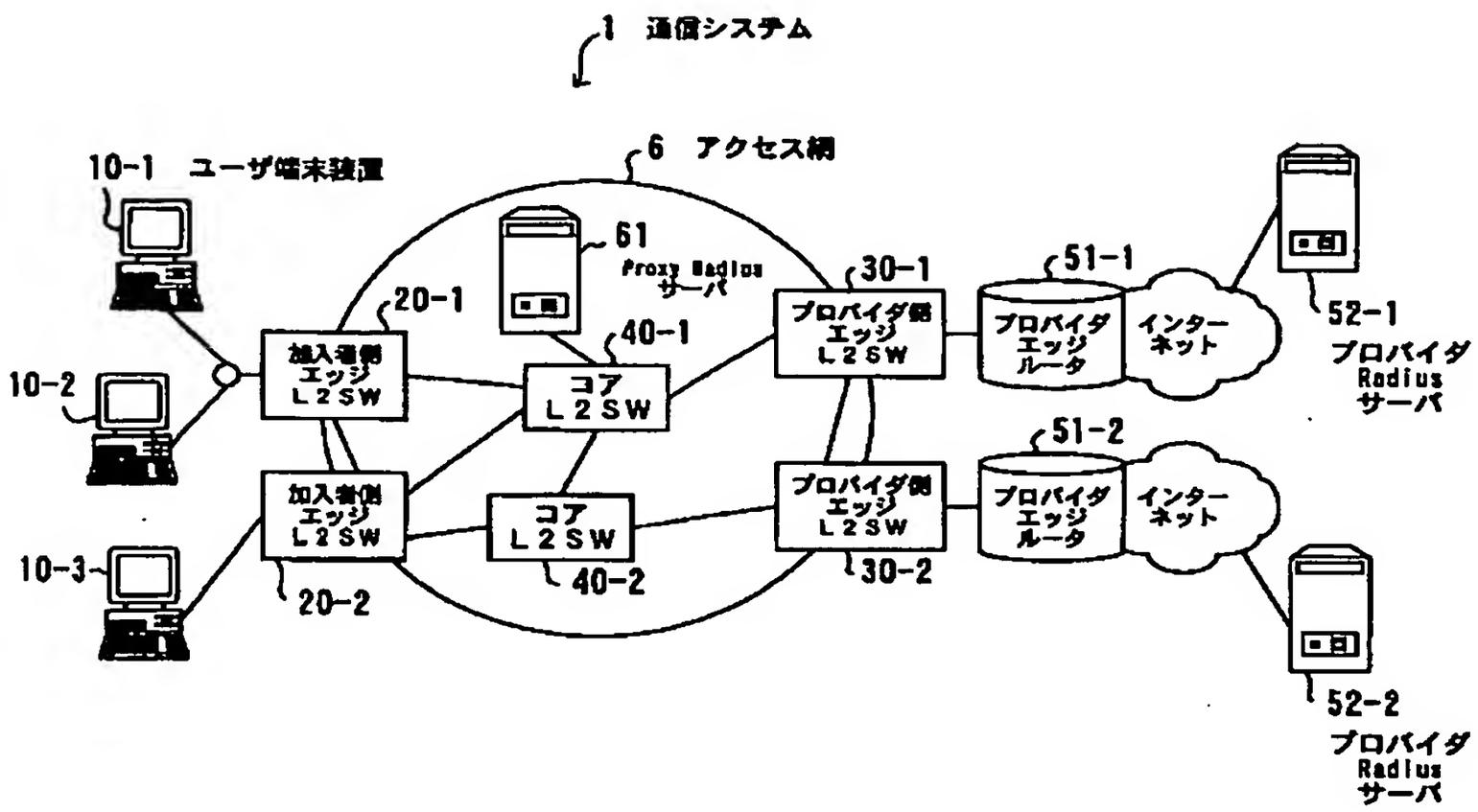



【図4】

| 0 | | | 31 |
|---|---|---|---|
| DESTINATION ADDR | | | |
| DESTINATION ADDR | | SOURCE ADDR | |
| SOURCE ADDR | | | |
| ETHER TYPE(=0x0800) | VER | IHL | TOS |
| TOTAL LENGTH | FLAGS | FRAGMENT OFFSET | |
| TTL | PROTOCOL | HEADER CHECKSUM | |
| SOURCE IP ADDR | | | |
| DESTINATION IP ADDR | | | |
| OPTIONS | | | PADDING |

IHL:Internet Header Length
TOS:Type Of Service
TTL:Time To Live

【図3】




【図5】

| 0 | | 31 |
|---|---|---|
| DESTINATION ADDR | | |
| DESTINATION ADDR | SOURCE ADDR | |
| SOURCE ADDR | | |
| TPID(=0x8100) | PRI CFI | VID(=1～4094) |
| ETHER TYPE(=0x0800) | IP PACKET… | |

TPID:Tag Protocol Identifier
PRI :Priority
CFI :Canonical Format Indicator
VID :VLAN Identifier

【図7】

T2a セッション管理テーブル

| MACアドレス | セッションID | 状態 | ネゴシエーションパラメータ |
|---|---|---|---|
| A | 0x1234 | IP通信フェーズ | VLAN-ID=10、割当IPアドレス=a、xSP-IPアドレス=X |
| B | 0x5678 | IP通信フェーズ | VLAN-ID=11、割当IPアドレス=b、xSP-IPアドレス=y |
| C | 0x7777 | 認証フェーズ | VLAN-ID=12(IPアドレスはネゴシエーション中のため未設定) |
| D | 0x3859 | IP通信フェーズ | VLAN-ID=11、割当IPアドレス=d、xSP-IPアドレス=y |
| ---- | ---- | ---- | ---- |

【図8】

T2b MAC-VIDテーブル

| MACアドレス | セッションID | VLAN-ID |
|---|---|---|
| A | 0x1234 | 10 |
| B | 0x5678 | 11 |
| | | |
| D | 0x3859 | 11 |
| ---- | ---- | ---- |

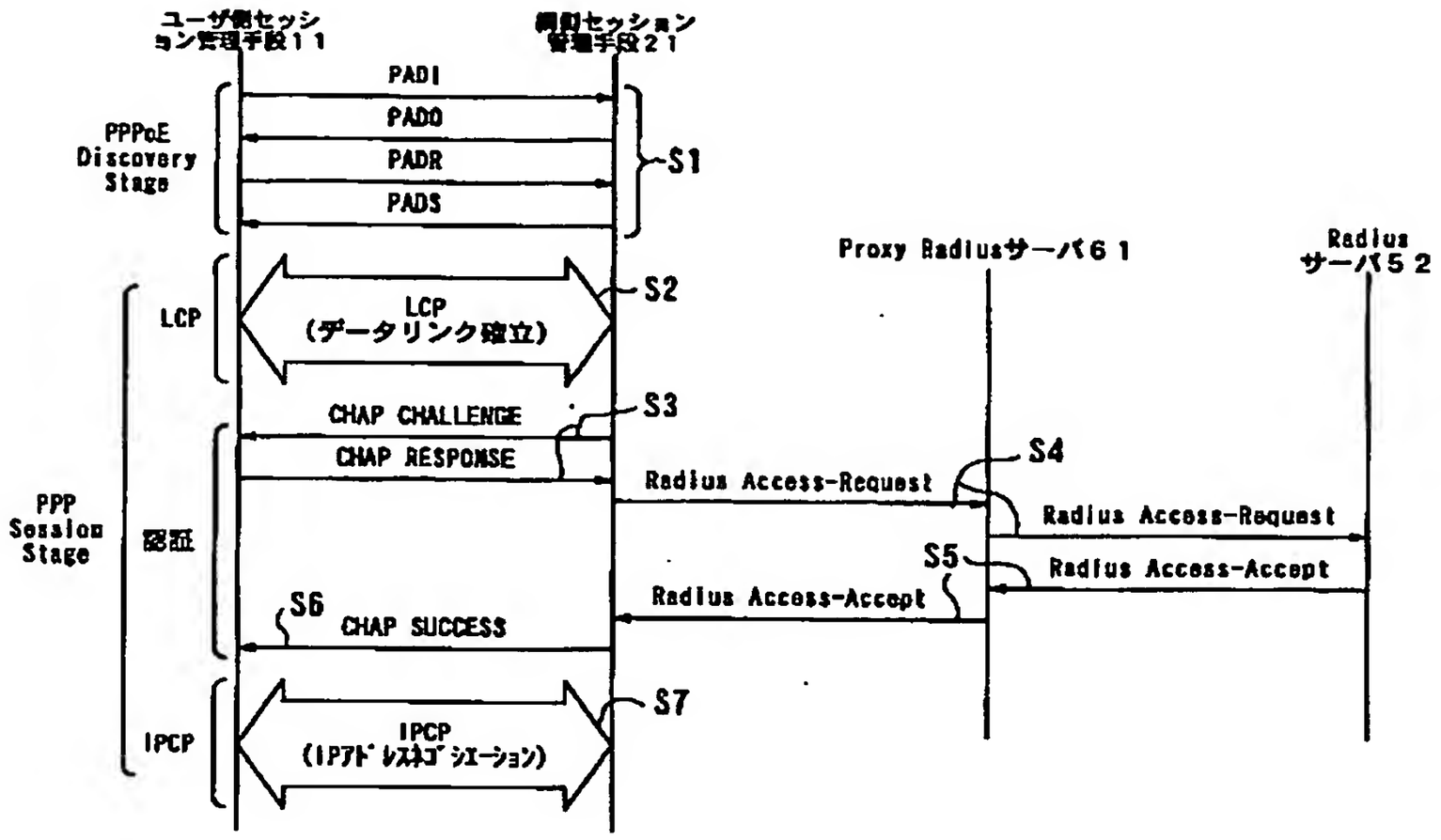
← Cは認証フェーズ中であるため未登録

【図10】

T2d ポート属性テーブル

| ポート番号 | 受信フレーム | ブロードキャストフィルタリング | タグ挿抜 |
|---|---|---|---|
| 1 | PPPoE、IP、ARP | ON | UnTag |
| 2 | PPPoE、IP、ARP | ON | UnTag |
| 3 | PPPoE、IP、ARP | ON | UnTag |
| 4 | PPPoE、IP、ARP | ON | UnTag |
| 5 | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 6 | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 7 | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| ---- | ---- | ---- | ---- |

【図6】




【図9】

T2c フォワーディングテーブル

For VLAN-ID=10

| MAC アドレス | 出力ポート |
|---|---|
| A | 1 |
| X | 5 |
| ---- | ---- |

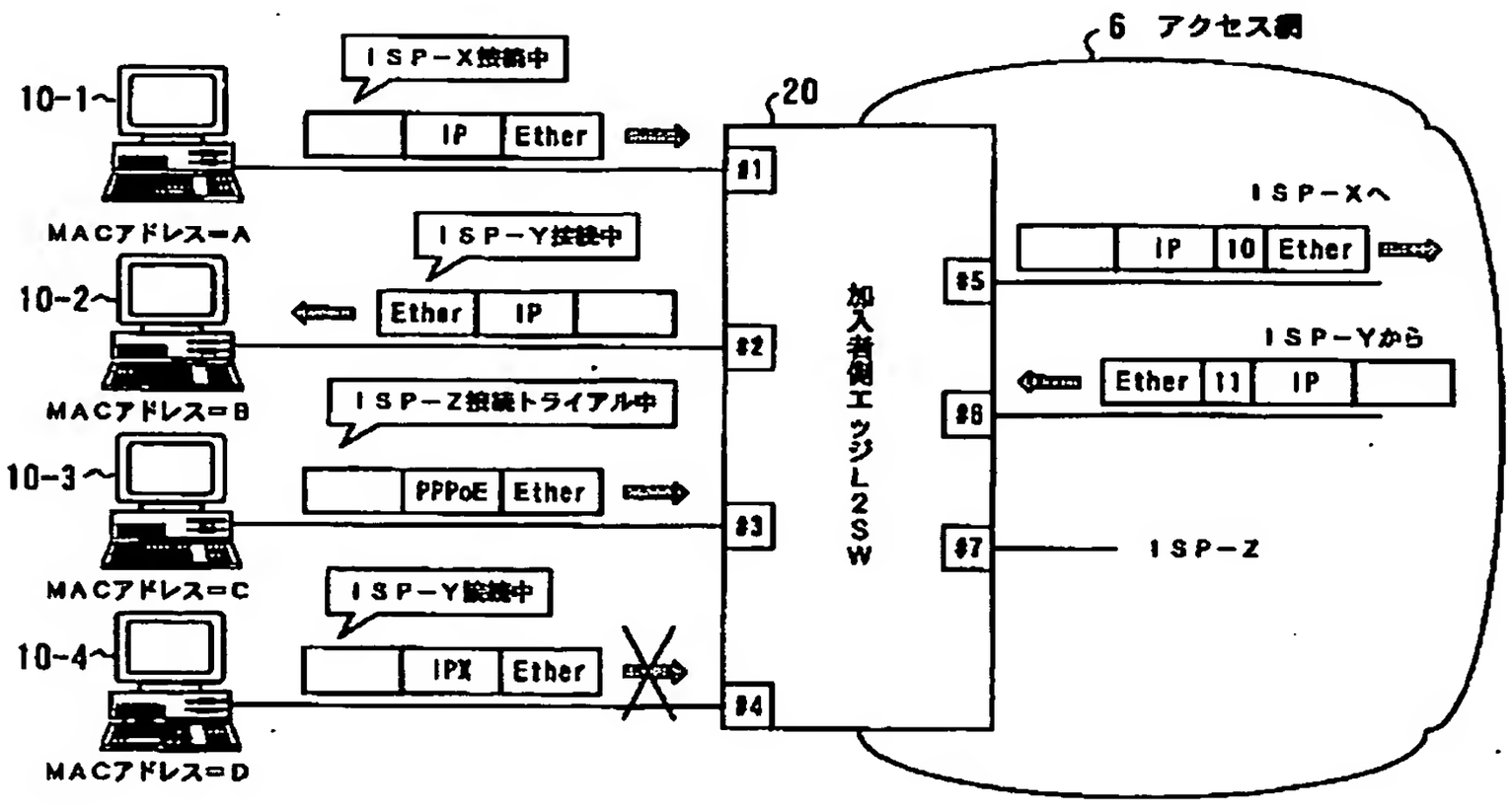
For VLAN-ID=11

| MAC アドレス | 出力ポート |
|---|---|
| B | 2 |
| D | 4 |
| Y | 6 |
| ---- | ---- |

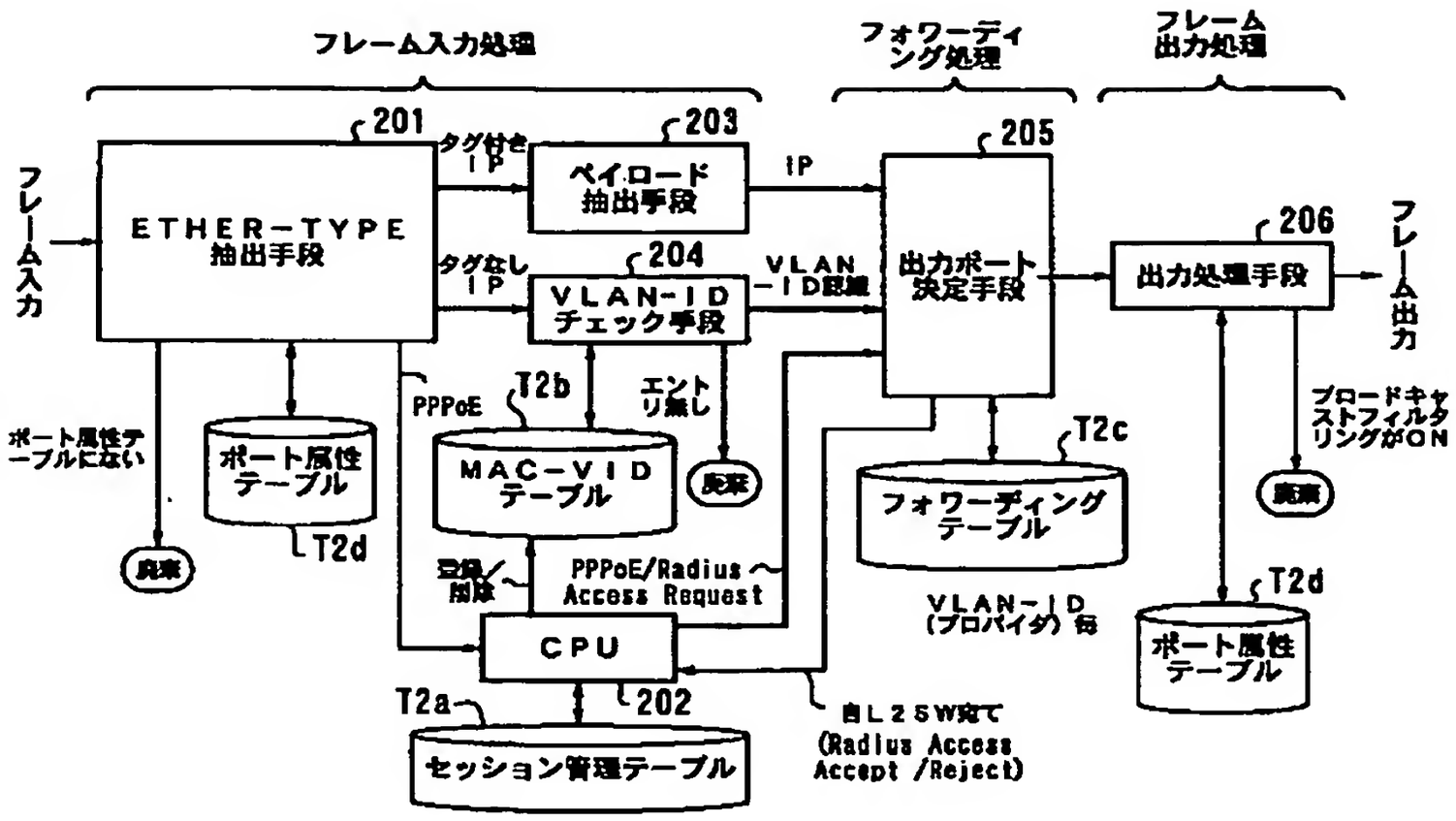
For VLAN-ID=12

| MAC アドレス | 出力ポート |
|---|---|
| C | 3 |
| Z | 7 |
| ---- | ---- |

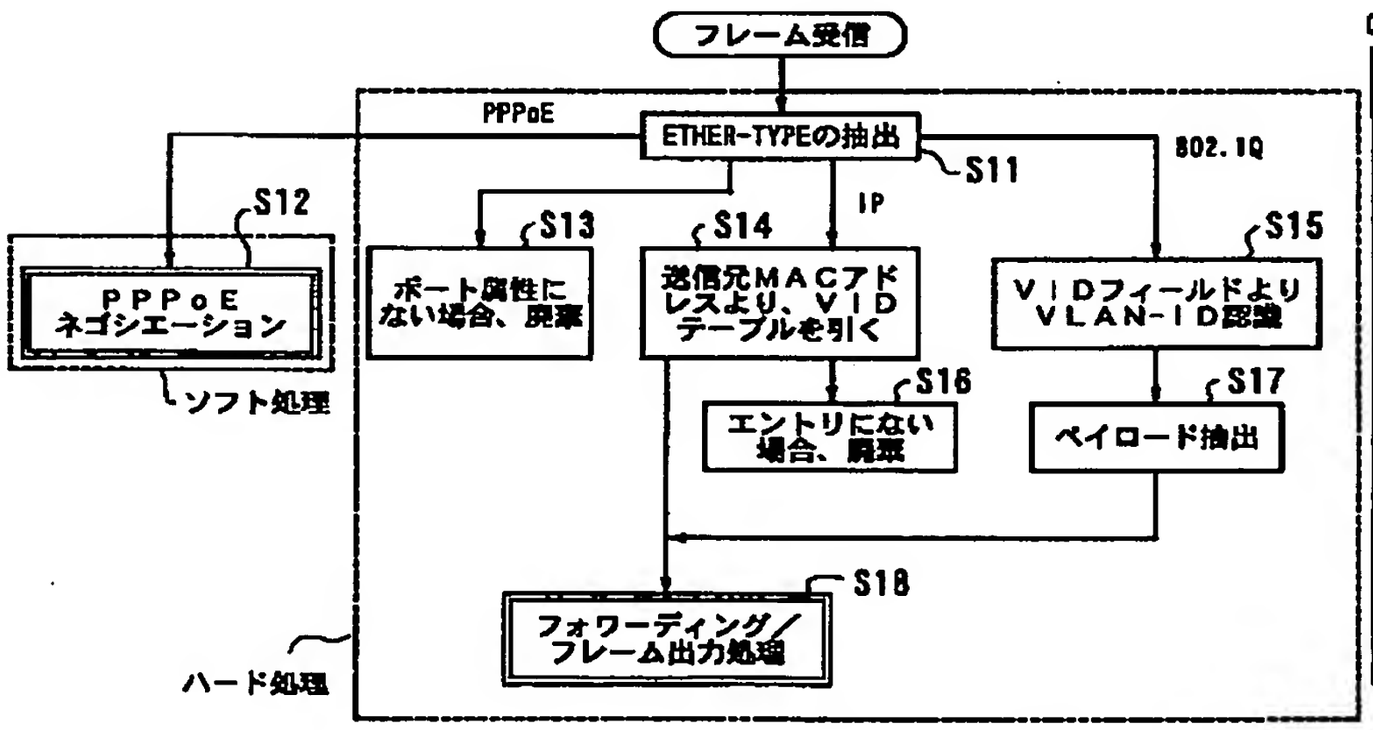
【図11】



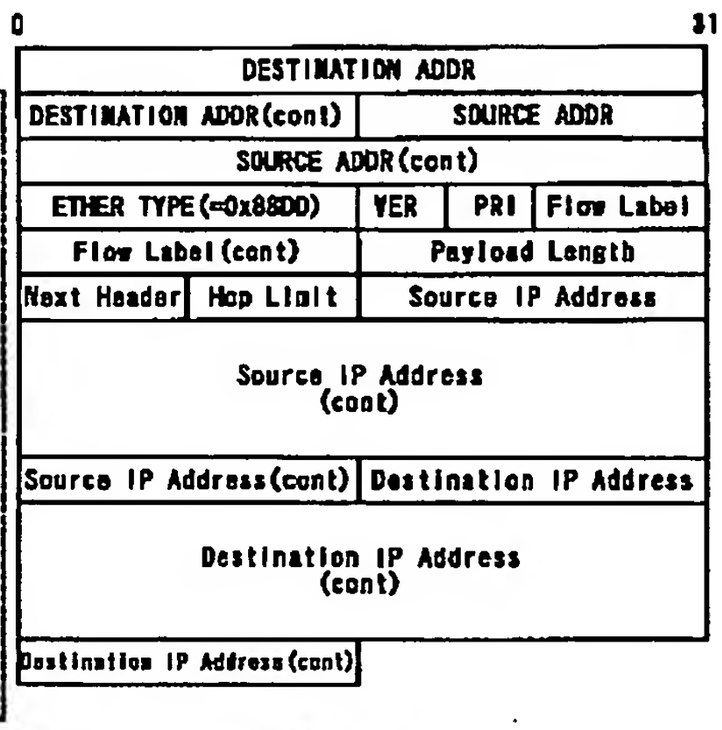
【図１２】




【図１３】

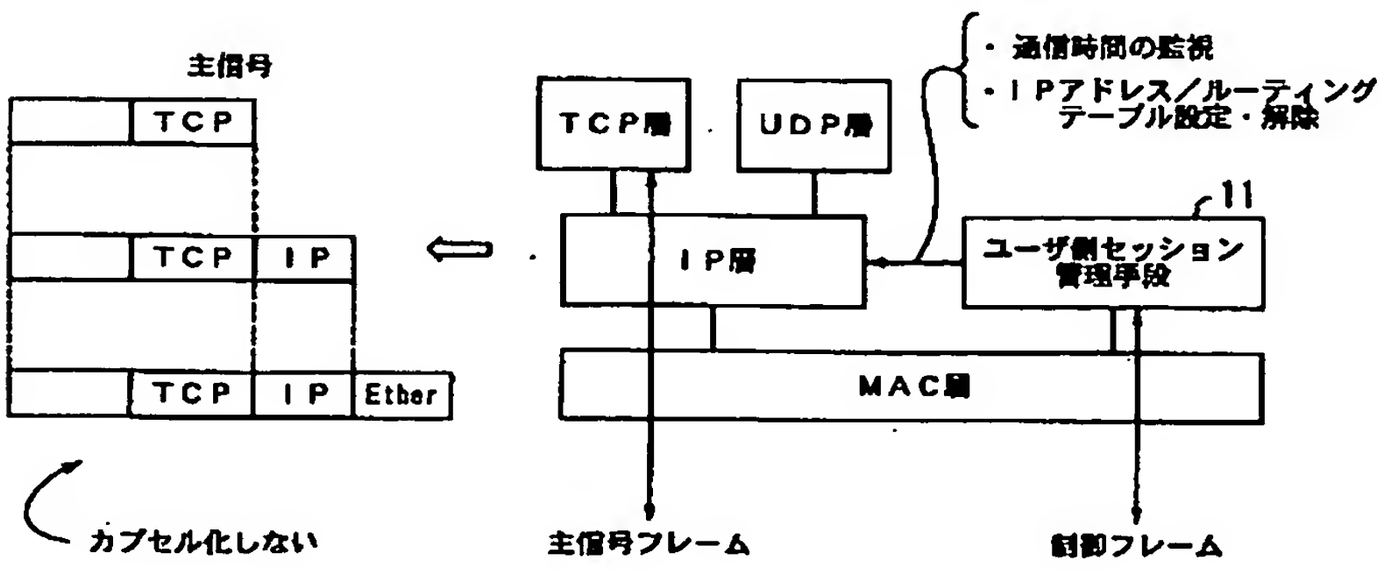



【図２９】

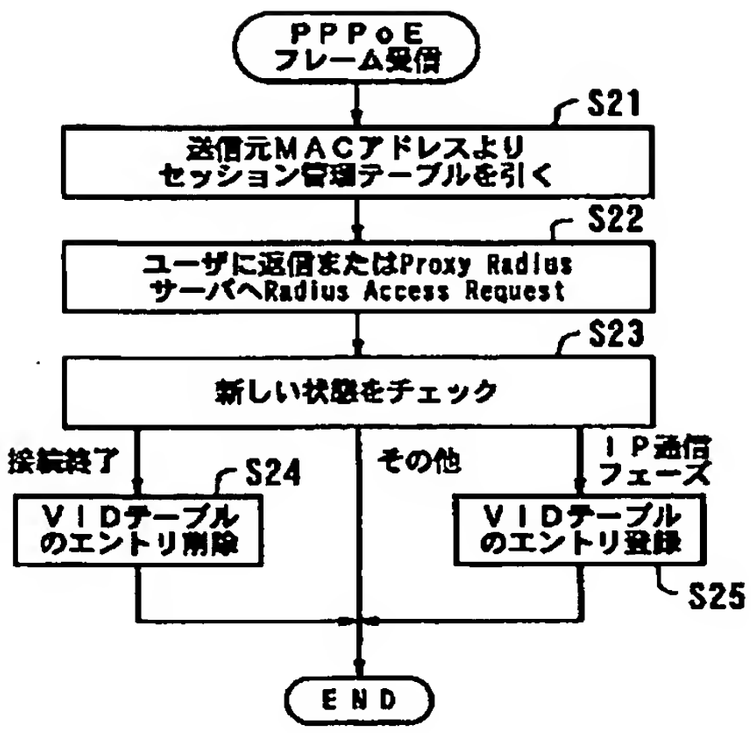



ＩＰｖ６データフォーマット

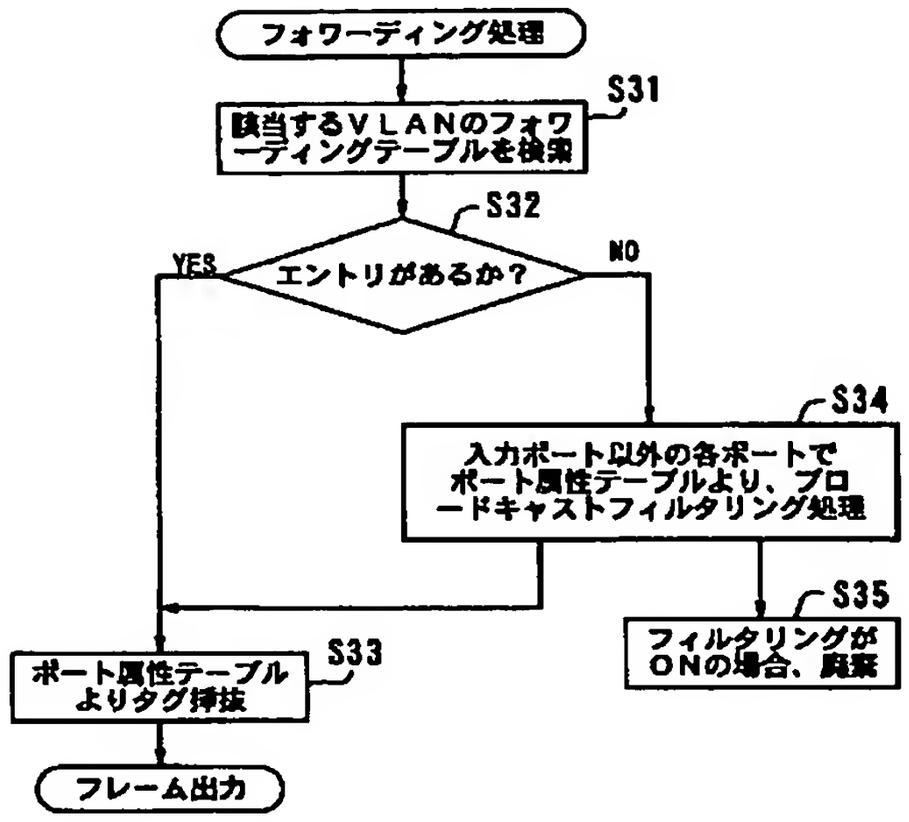
【図１６】



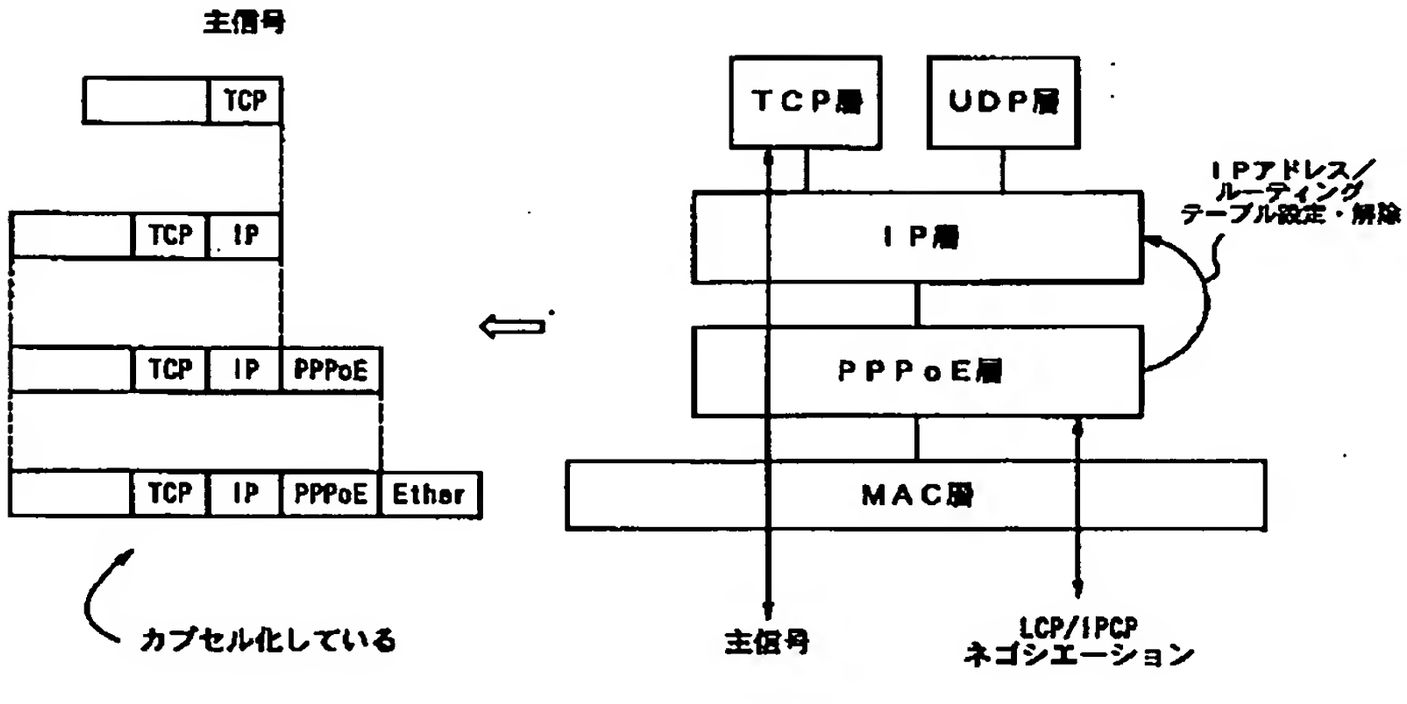
【図14】




【図15】




【図17】




【図18】

(接続前)

| MAC アドレス | セッション ID | 状態 | ネゴシエーションパラメータ |
|---|---|---|---|
| ? | 0x0000 | 接続トライアル | ユーザID：ユーザ名@プロバイダ名、パスワード |

接続先が一意に固定の場合は、
あらかじめ記憶させておくことも可能

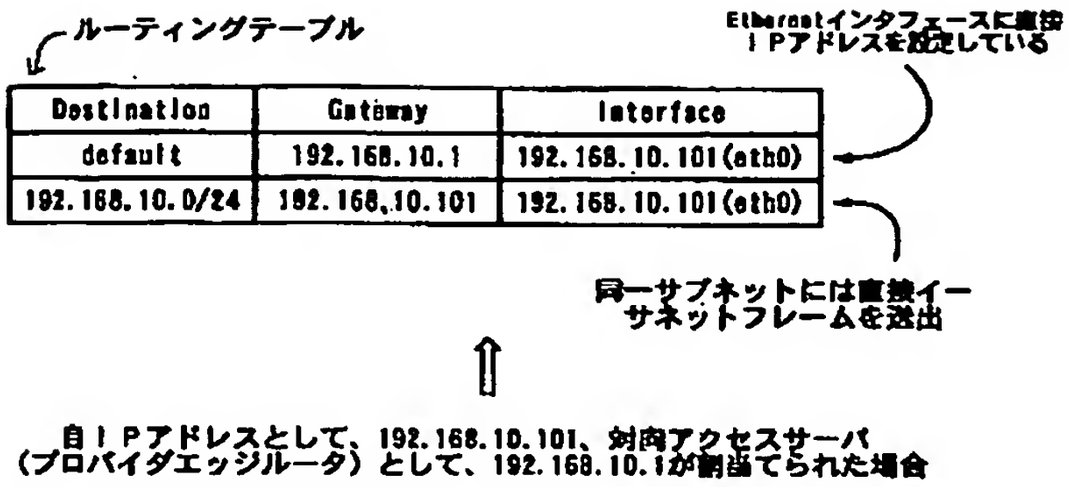
(接続後)

| MAC アドレス | セッション ID | 状態 | ネゴシエーションパラメータ |
|---|---|---|---|
| M | 0x1234 | IP通信フェーズ | 割当IPアドレス＝a、プロバイダーIPアドレス＝x |

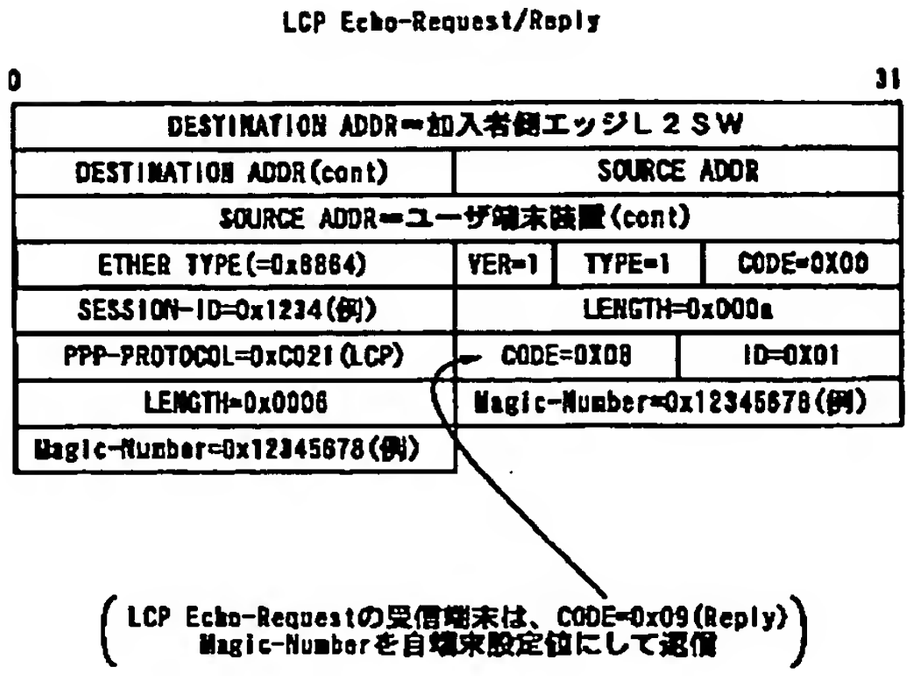
加入者側エッジL2SW
のMACアドレス

aを自Ethernetインタフェースの IPアドレスに設定
xをデフォルトルートに設定

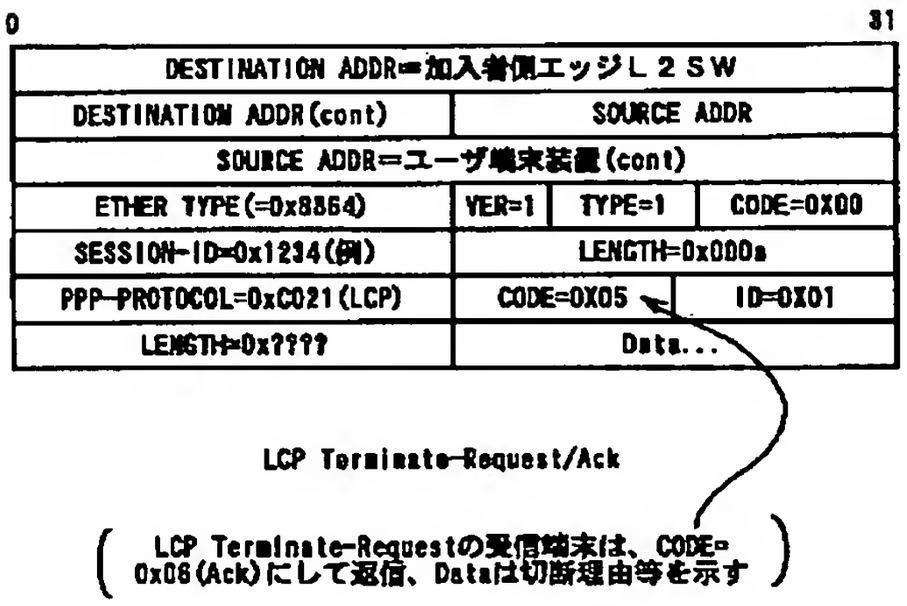
【図19】



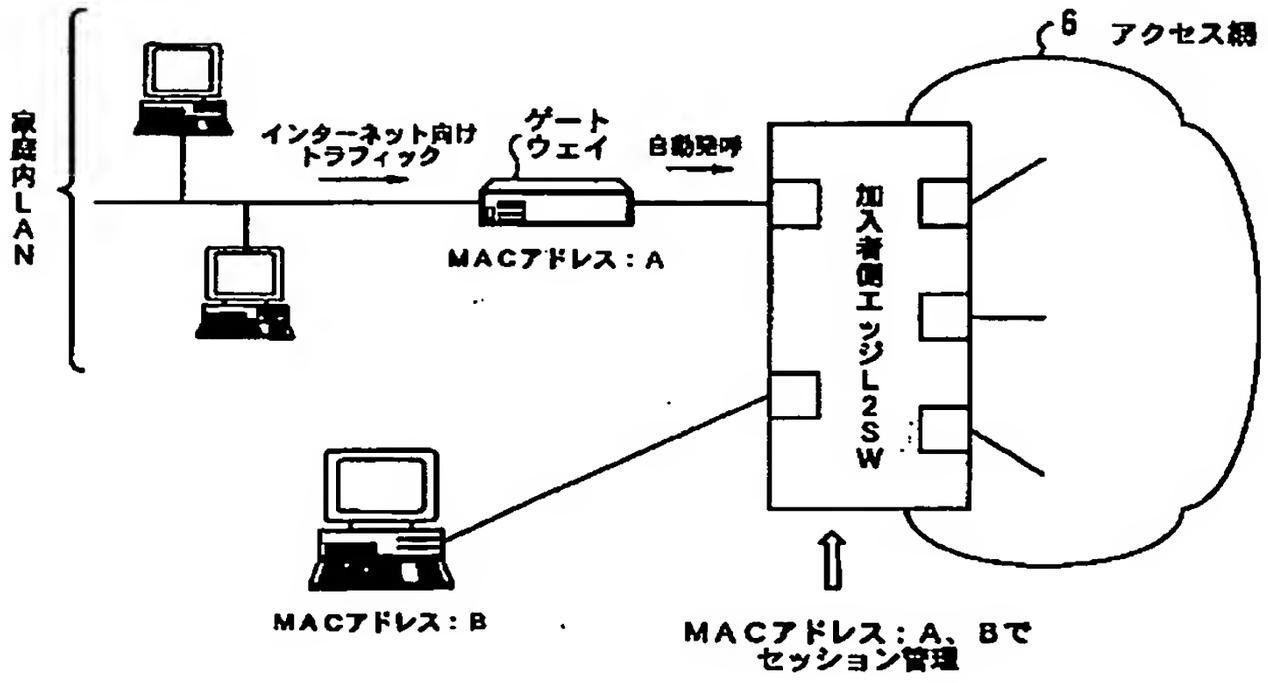

【図20】



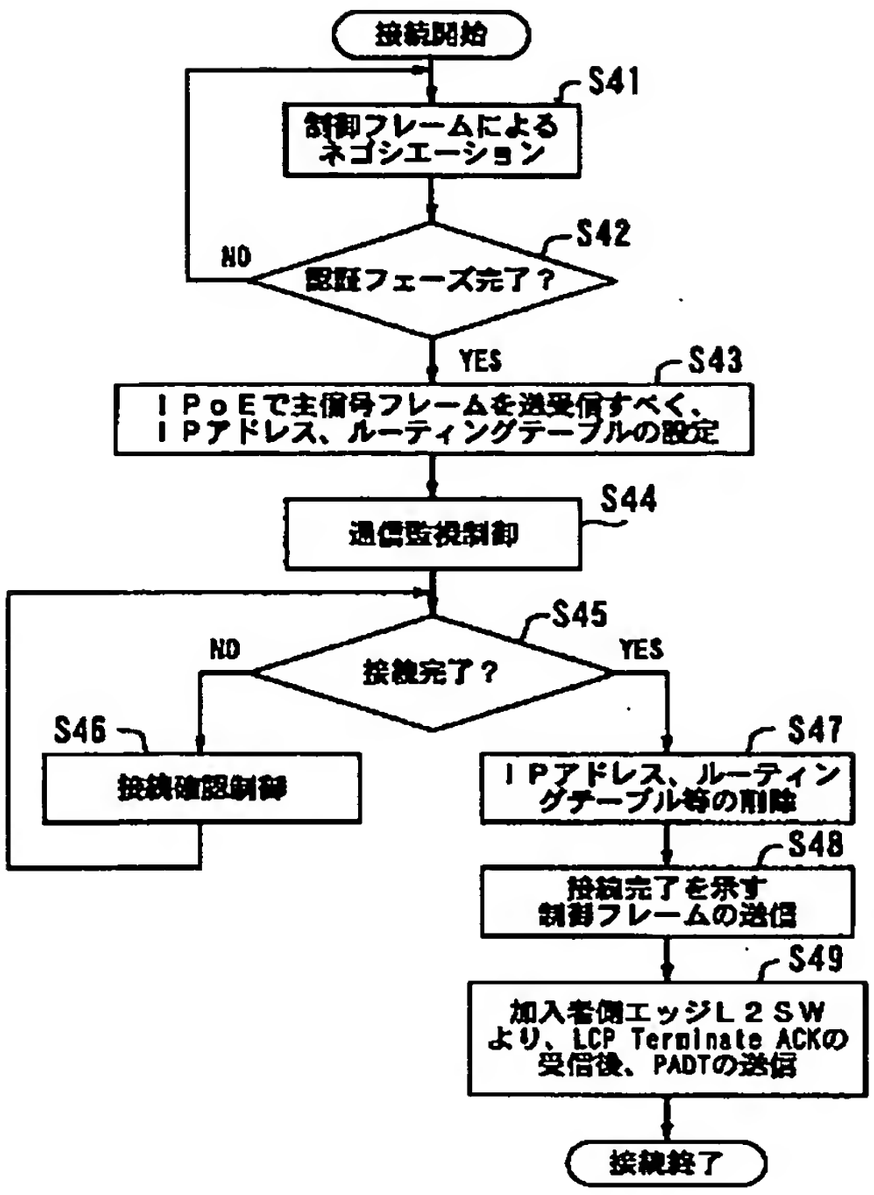

【図21】



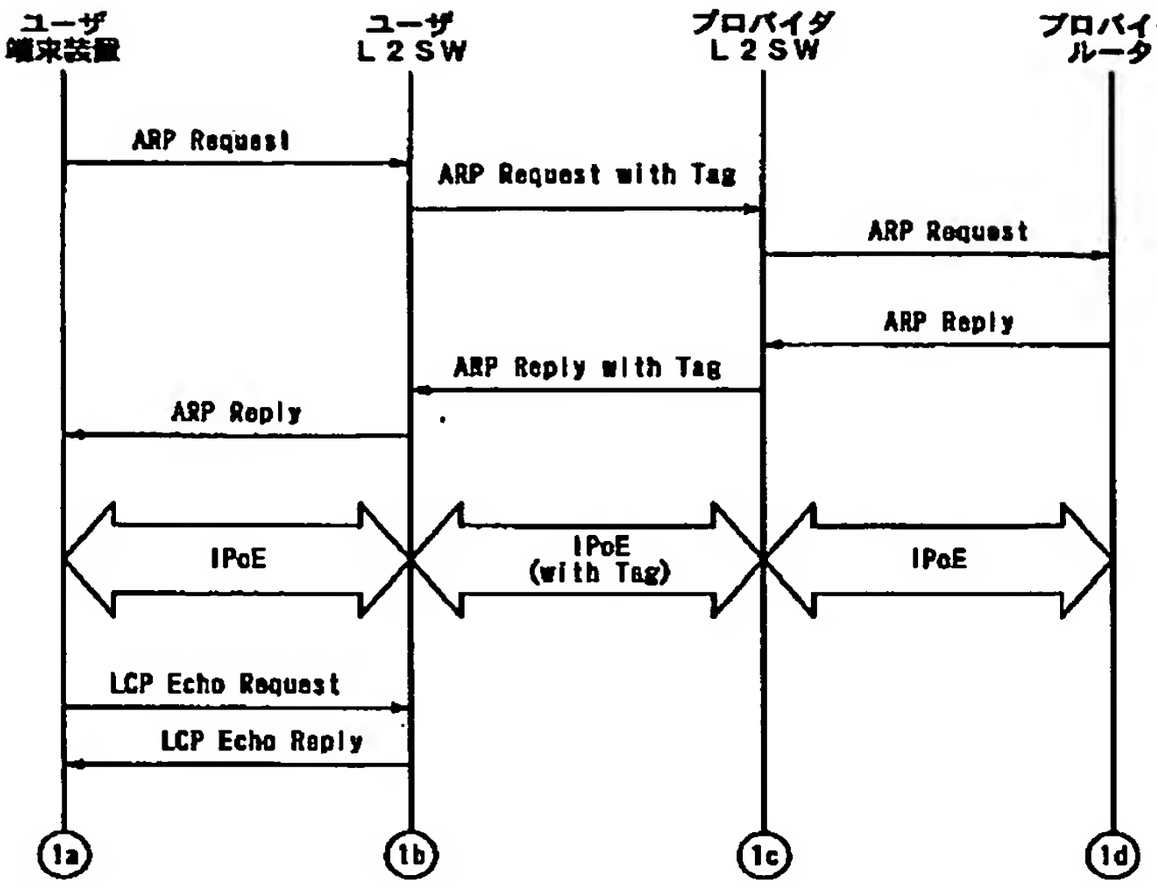

【図22】



【図23】




【図33】




【図24】

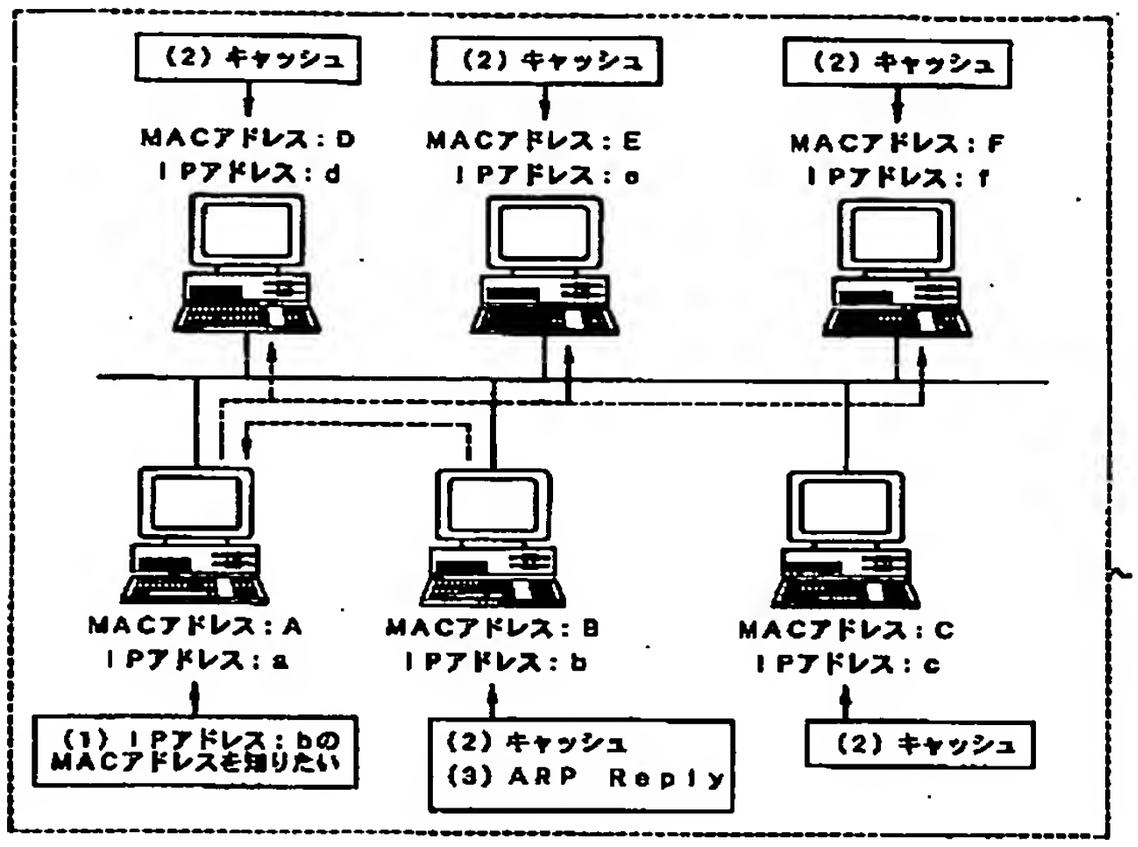
| DESTINATION ADDR | ff:ff:ff:ff:ff:ff | A |
|---|---|---|
| SOURCE ADDR | A | B |
| Ether Type=0x806 | 0x0806 | 0x0806 |
| Hw Addr Type=0x0001 | | |
| Prot Addr Type=0x800 | | |
| Hw Addr Len=6 | | |
| Prot Addr Len=4 | | |
| Code | 0x01(Req) | 0x02(Reply) |
| Src Hw Addr | A | B |
| Src Prot Addr | a | b |
| Tgt Hw Addr | ?(知りたい) | A |
| Tgt Prot Addr | b | a |
| FCS | | |
| ARP Packet | ARP Request | ARP Reply |

受信端末は
キャッシュ

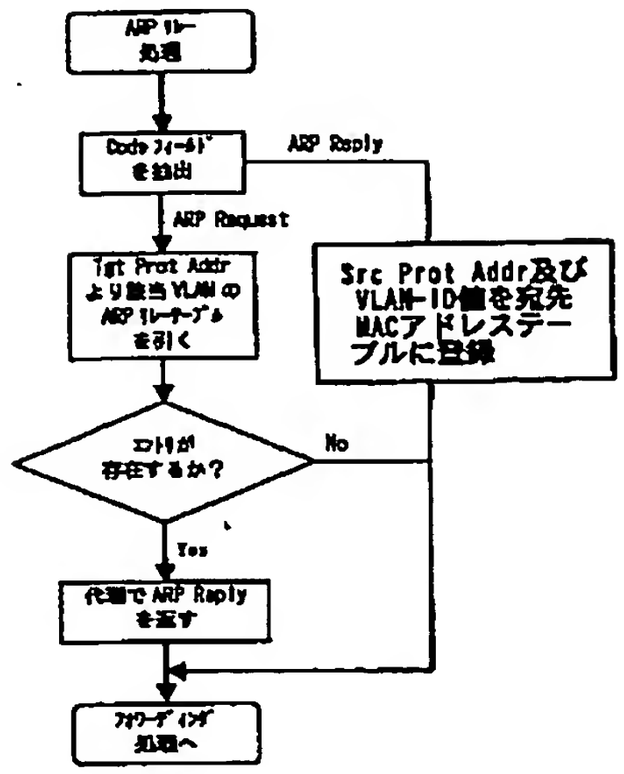
【図40】

| プロバイダ名 | ＶＬＡＮ－ＩＤ | プロバイダＲａｄｉｕｓ サーバ情報 |
|---|---|---|
| ＩＳＰ－Ｘ | １０ | ＩＰアドレス＝ｘ１ |
| ＩＳＰ－Ｙ | １１ | ＩＰアドレス＝ｙ１ |
| ＩＳＰ－Ｚ | １２ | ＩＰアドレス＝ｚ１ |

【図25】




【図46】




【図26】

セッション管理テーブル

| MACアドレス | セッションID | 状態 | ネゴシエーションパラメータ |
|---|---|---|---|
| A | 0x1234 | IP通信フェーズ | VLAN-ID=10、割当IPアドレス=a、xSP-IPアドレス=X |
| B | 0x5678 | IP通信フェーズ | VLAN-ID=11、割当IPアドレス=b、xSP-IPアドレス=y |
| C | 0x7777 | 認証フェーズ | VLAN-ID=12(IPアドレスはネゴシエーション中のため未設定) |
| D | 0x3859 | IP通信フェーズ | VLAN-ID=11、割当IPアドレス=d、xSP-IPアドレス=y |
| --- | ---- | --- | --- |

⇩

| IPアドレス | MACアドレス |
|---|---|
| a | A |
| --- | --- |

For VLAN-ID=10

| IPアドレス | MACアドレス |
|---|---|
| b | B |
| d | D |

For VLAN-ID=11

認証フェーズ完了時に登録

| IPアドレス | MACアドレス |
|---|---|
| | ? |
| --- | --- |

For VLAN-ID=12

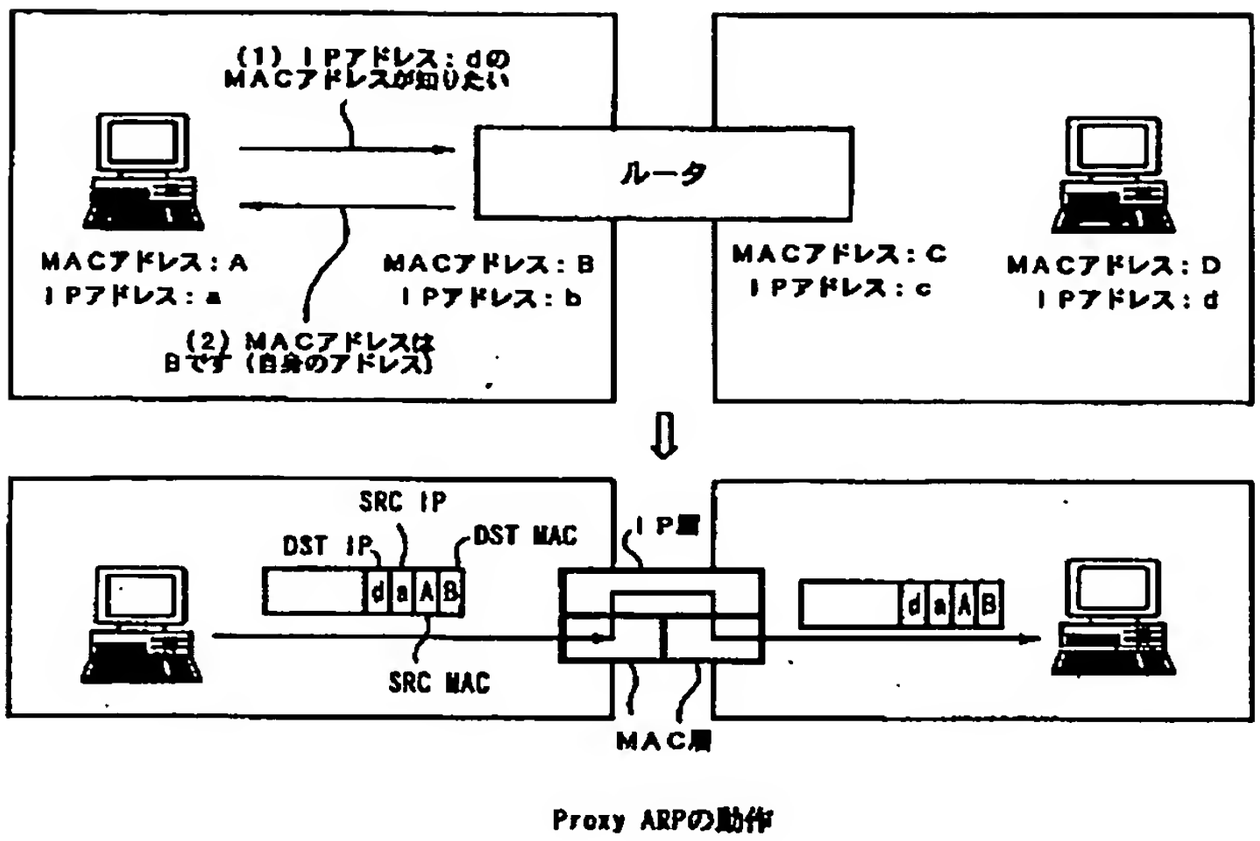
ARPリレーテーブル（VLAN－IDごとに独立）

【図42】

| MACアドレス | セッションID | 状態 | ネゴシエーションパラメータ |
|---|---|---|---|
| A | 0x1234 | IP通信フェーズ | VLAN-ID=10、割当IPアドレス=a、xSP-IPアドレス=X |
| A | 0x5678 | IP通信フェーズ | VLAN-ID=11、割当IPアドレス=b、xSP-IPアドレス=y |
| B | 0x7777 | 認証フェーズ | VLAN-ID=12(IPアドレスはネゴシエーション中のため未設定) |
| C | 0x3859 | IP通信フェーズ | VLAN-ID=11、割当IPアドレス=d、xSP-IPアドレス=y |
| --- | ---- | ---- | --- |

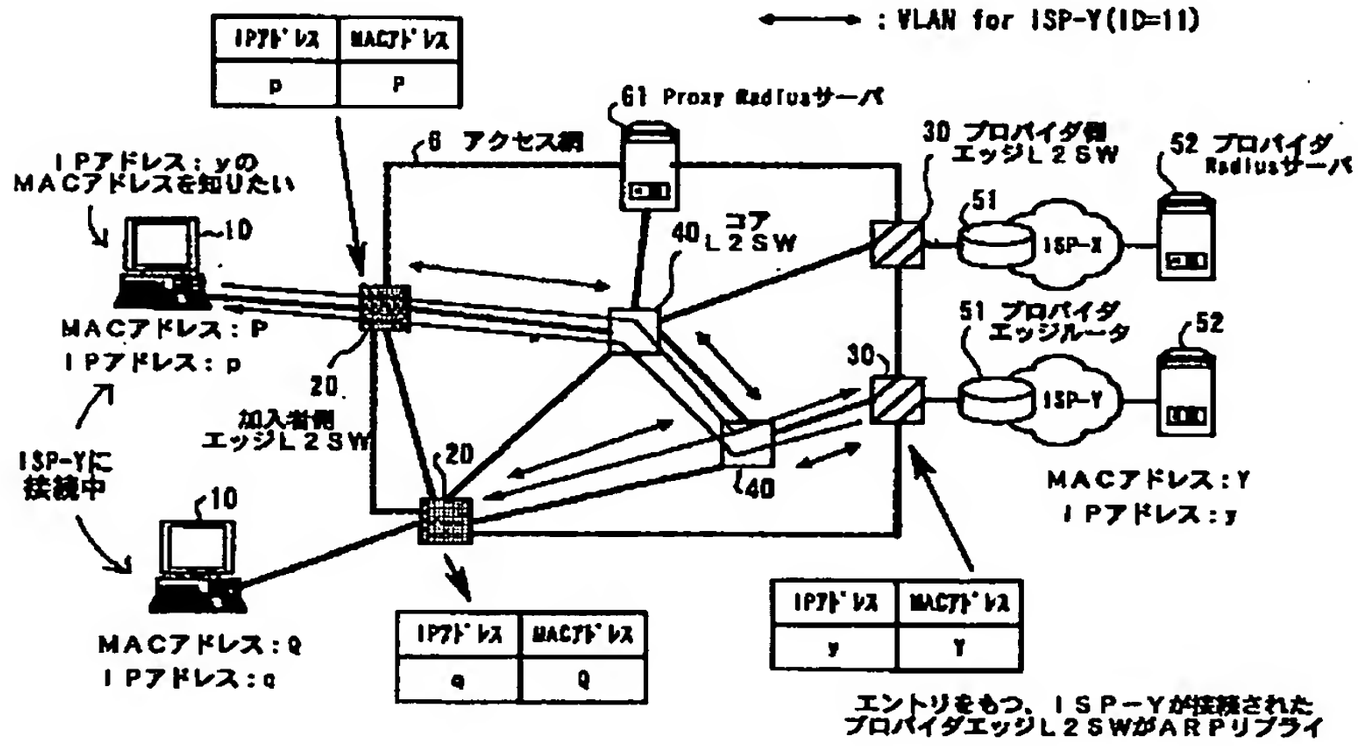
Aが複数同時接続中
ただし、送信元MACアドレス+セッションIDでセッションを一意に識別

【図27】

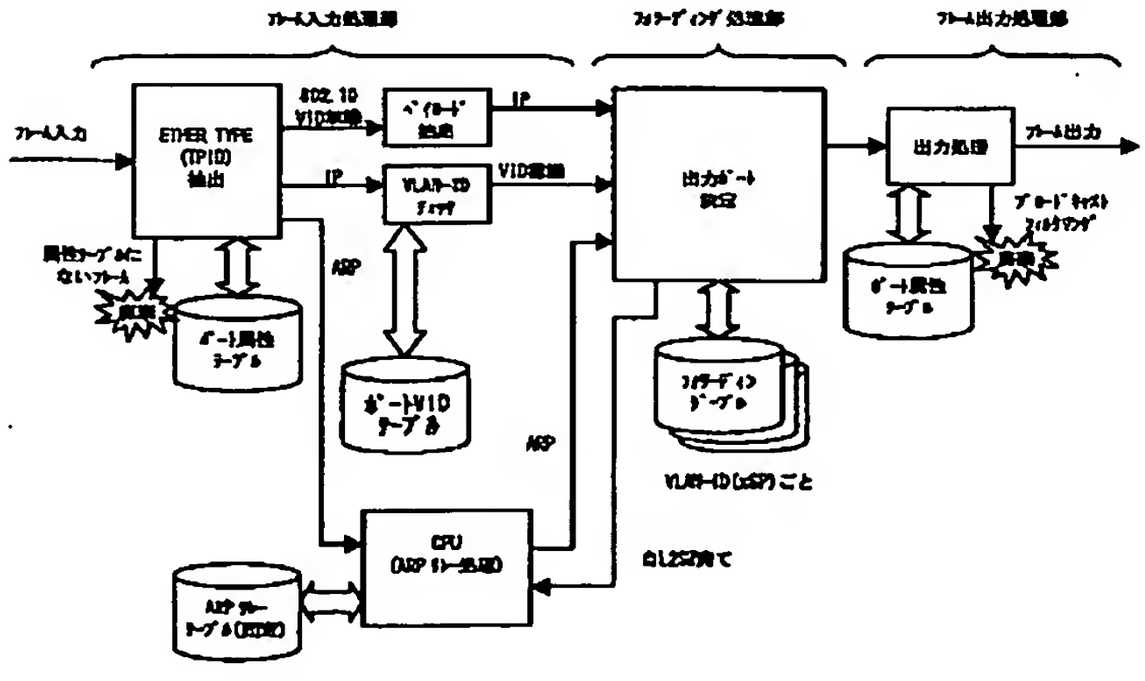



Proxy ARPの動作

【図28】



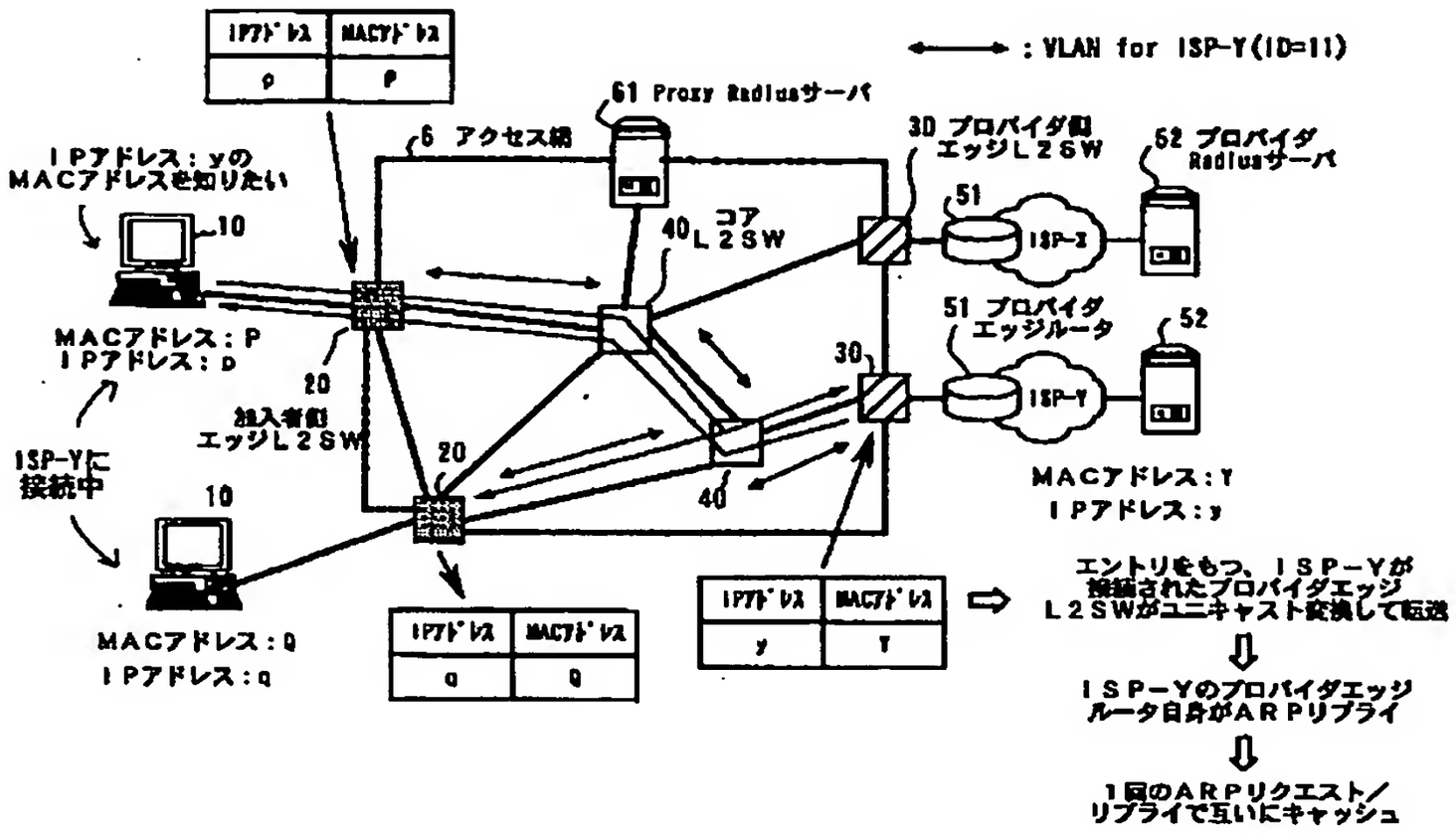

【図37】



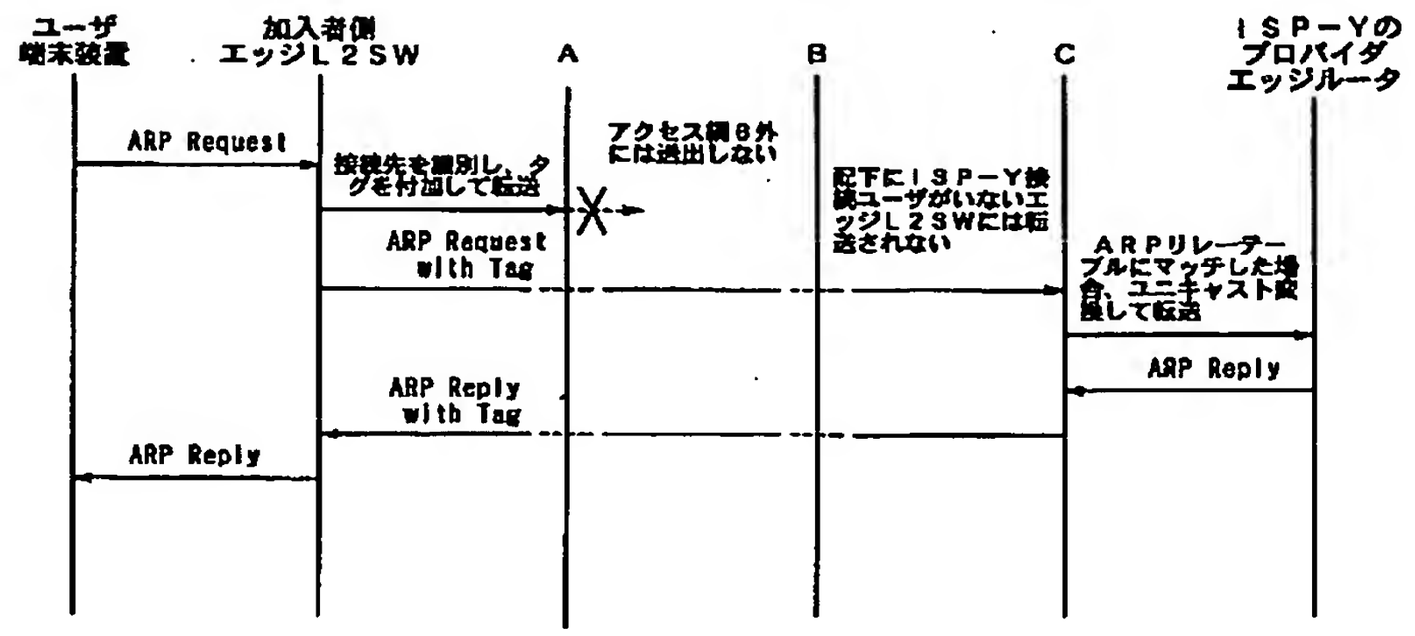

| IPサブネット | VLAN-ID |
|---|---|
| xxx. xxx. xxx. 0／24 | 10 |
| yyy. yyy. yyy. 0／24 | 11 |

IPサブネットテーブル

【図３０】

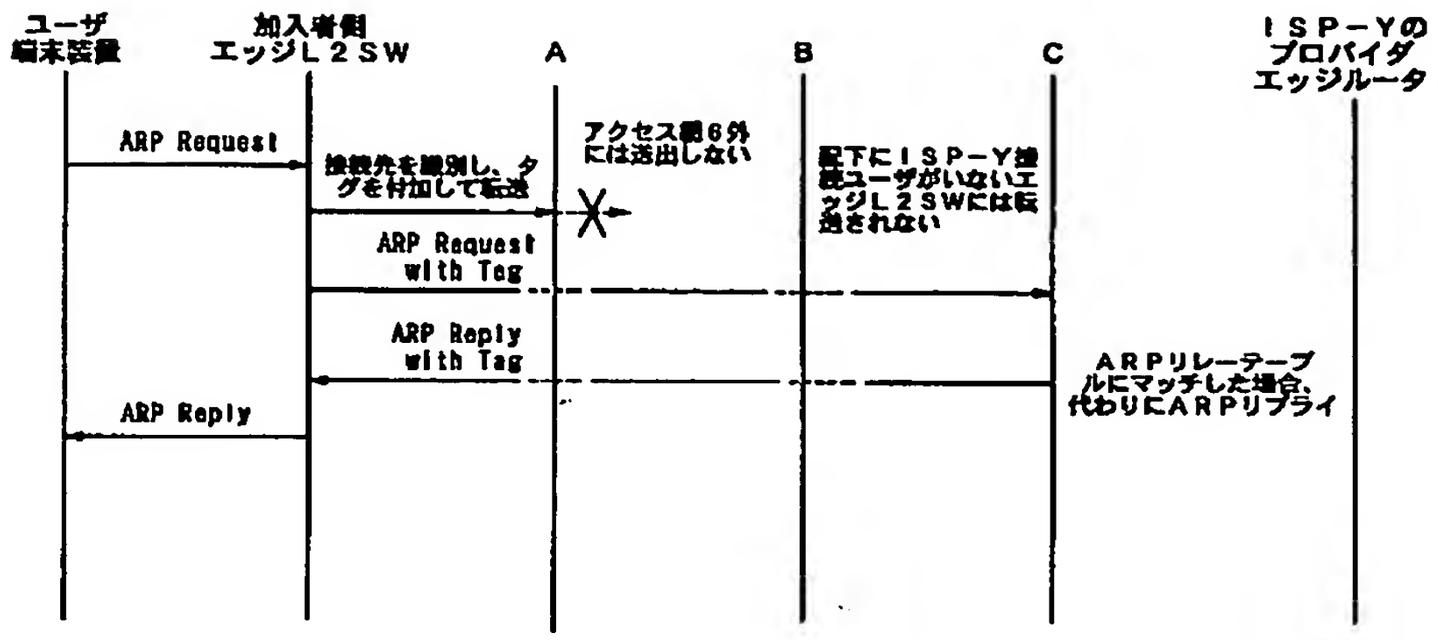



【図３１】



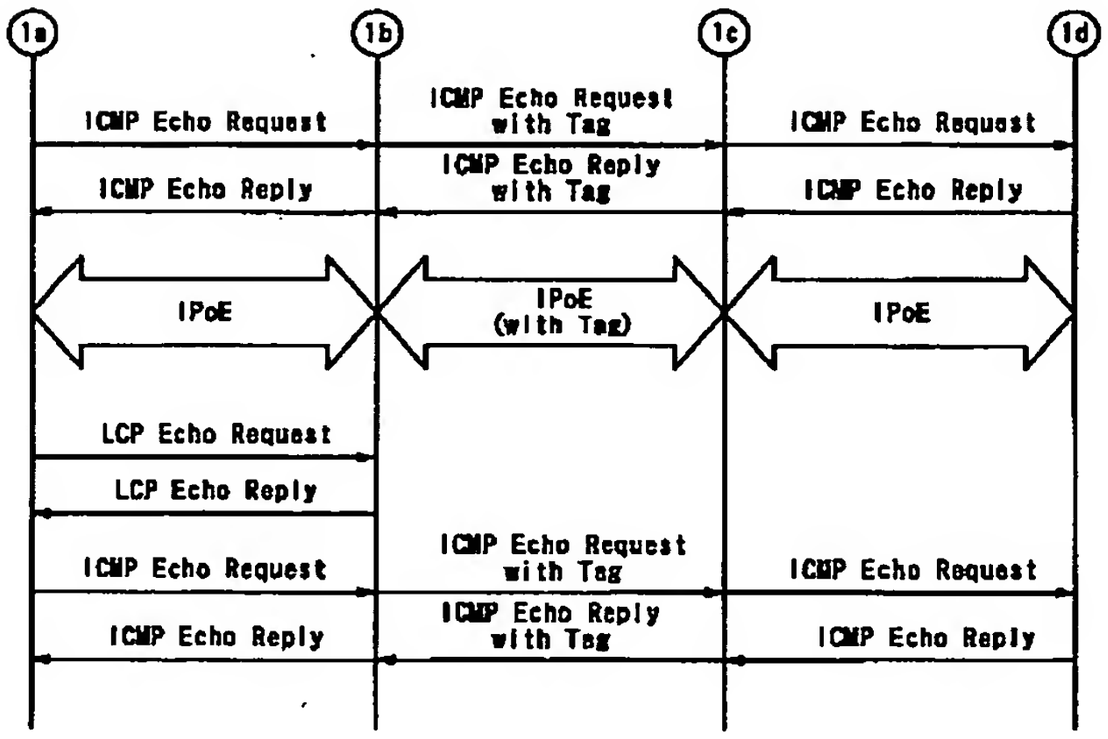

Ａ：プロバイダ側エッジＬ２ＳＷ：（ＩＳＰ－Ｙ接続ユーザが配下に存在する）
Ｂ：プロバイダ側エッジＬ２ＳＷ：（ＩＳＰ－Ｙ接続ユーザが配下に存在しない）
Ｃ：プロバイダ側エッジＬ２ＳＷ：（ＩＳＰ－Ｙが接続されている）

【図32】




A：プロバイダ側エッジL2SW：（ISP-Y接続ユーザが配下に存在する）
B：プロバイダ側エッジL2SW：（ISP-Y接続ユーザが配下に存在しない）
C：プロバイダ側エッジL2SW：（ISP-Yが接続されている）

【図34】




【図35】

| ポート | VLAN-ID |
|---|---|
| 5 | 10 |
| 6 | 11 |
| 7 | 12 |

固定値として登録
（ただし、プロバイダはIDについて登録する必要なし）

ポートVIDテーブル（プロバイダ側エッジL2SW）

| IP アドレス | MAC アドレス |
|---|---|
| x | X |

For VLAN-ID=10

| IP アドレス | MAC アドレス |
|---|---|
| y | Y |

For VLAN-ID=11

| IP アドレス | MAC アドレス |
|---|---|
| z | Z |

For VLAN-ID=12

固定値として登録

ARPリレーテーブル（プロバイダ側エッジL2SW）

| MACアドレス | 出力ポート |
|---|---|
| A | 1 |
| X | 5 |

For VLAN-ID=10

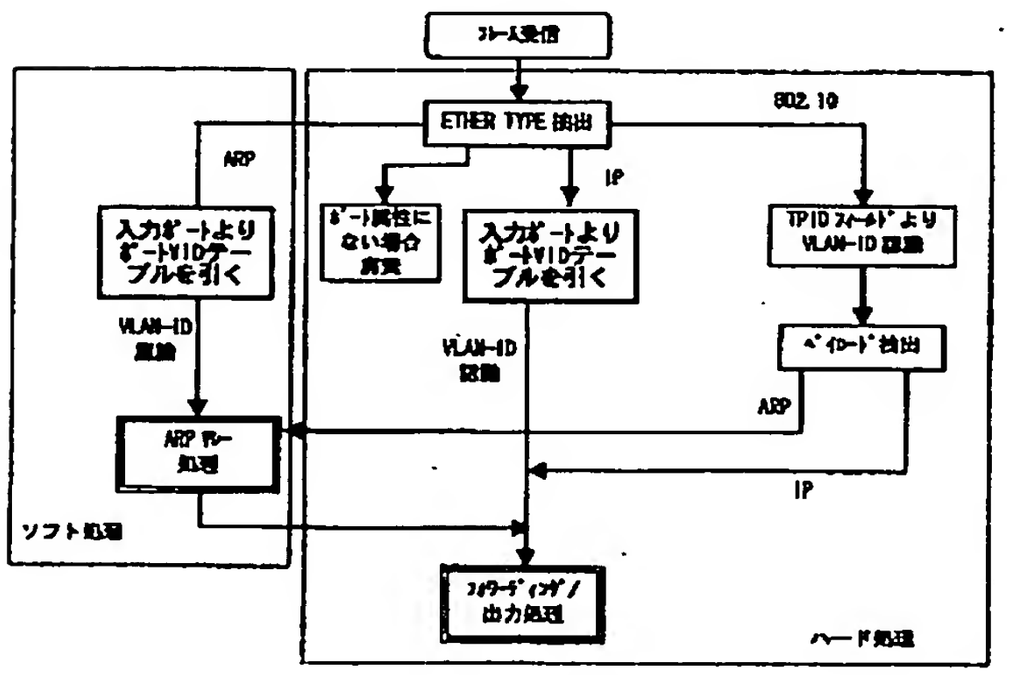
| MACアドレス | 出力ポート |
|---|---|
| B | 2 |
| D | 4 |
| Y | 6 |

For VLAN-ID=11

| MACアドレス | 出力ポート |
|---|---|
| C | 3 |
| Z | 7 |

For VLAN-ID=12

【図38】

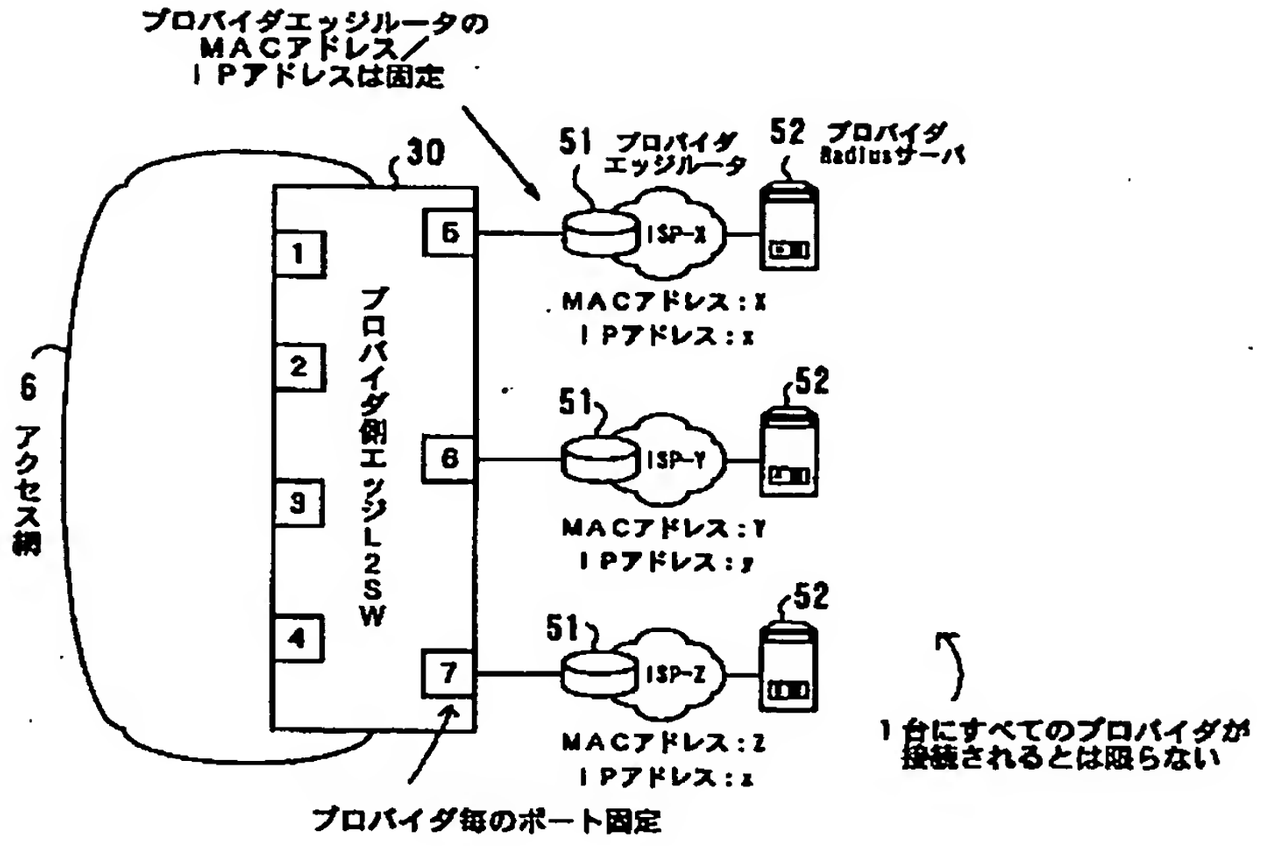



フォワーディングテーブル（VLAN-ID毎に独立）

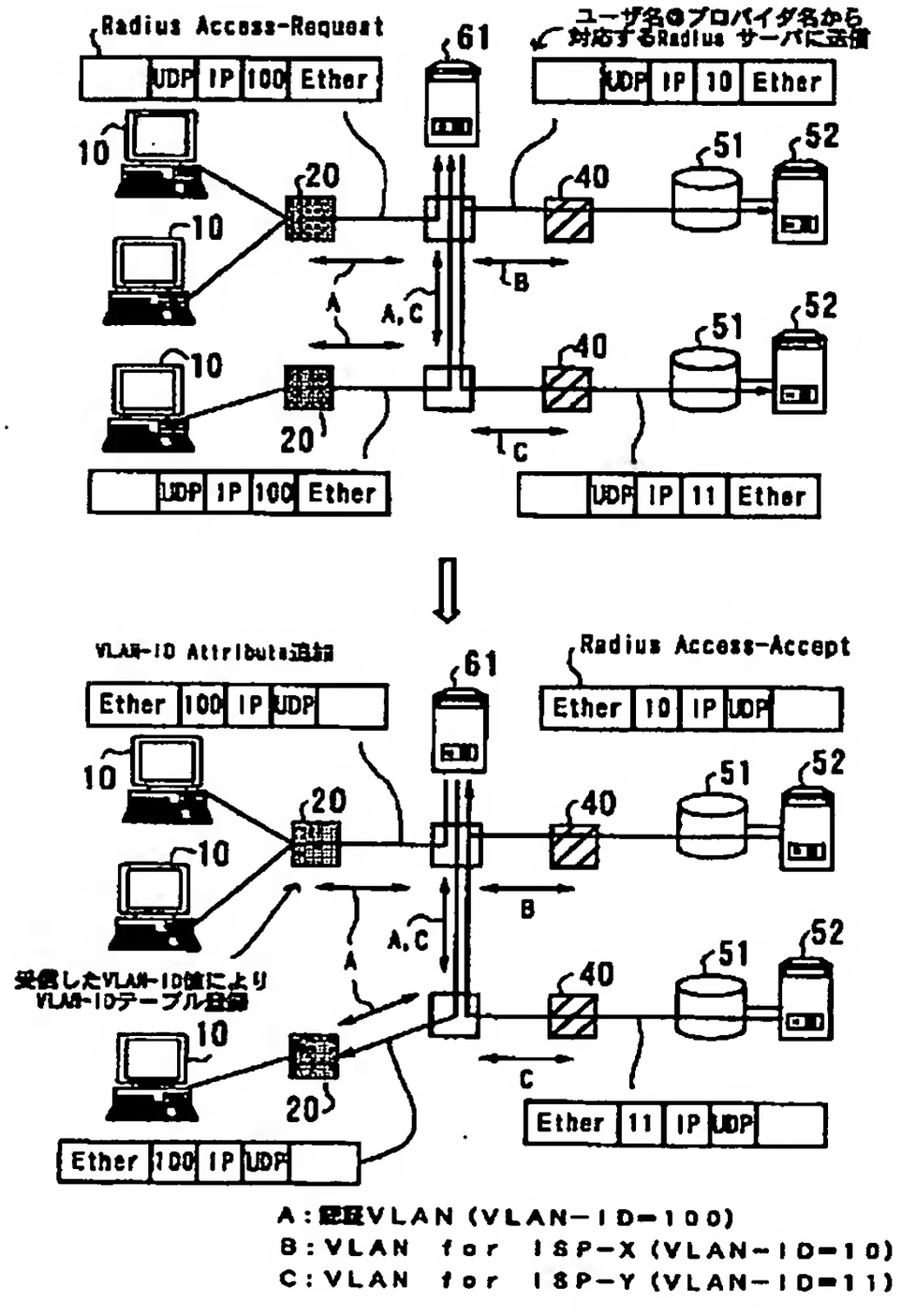
| ポート | 受信フレーム | ブロードキャストフィルタリング | タグ挿抜 |
|---|---|---|---|
| 1 | IEEEE802.1Q, GVRP, STP | OFF | With Tag |
| 2 | IEEEE802.1Q, GVRP, STP | OFF | With Tag |
| 3 | IEEEE802.1Q, GVRP, STP | OFF | With Tag |
| 4 | IEEEE802.1Q, GVRP, STP | OFF | With Tag |
| 5 | IP, ARP | ON | UnTag |
| 6 | IP, ARP | ON | UnTag |
| 7 | IP, ARP | ON | UnTag |

ポート属性テーブル（VLAN-ID毎に独立してもよい）

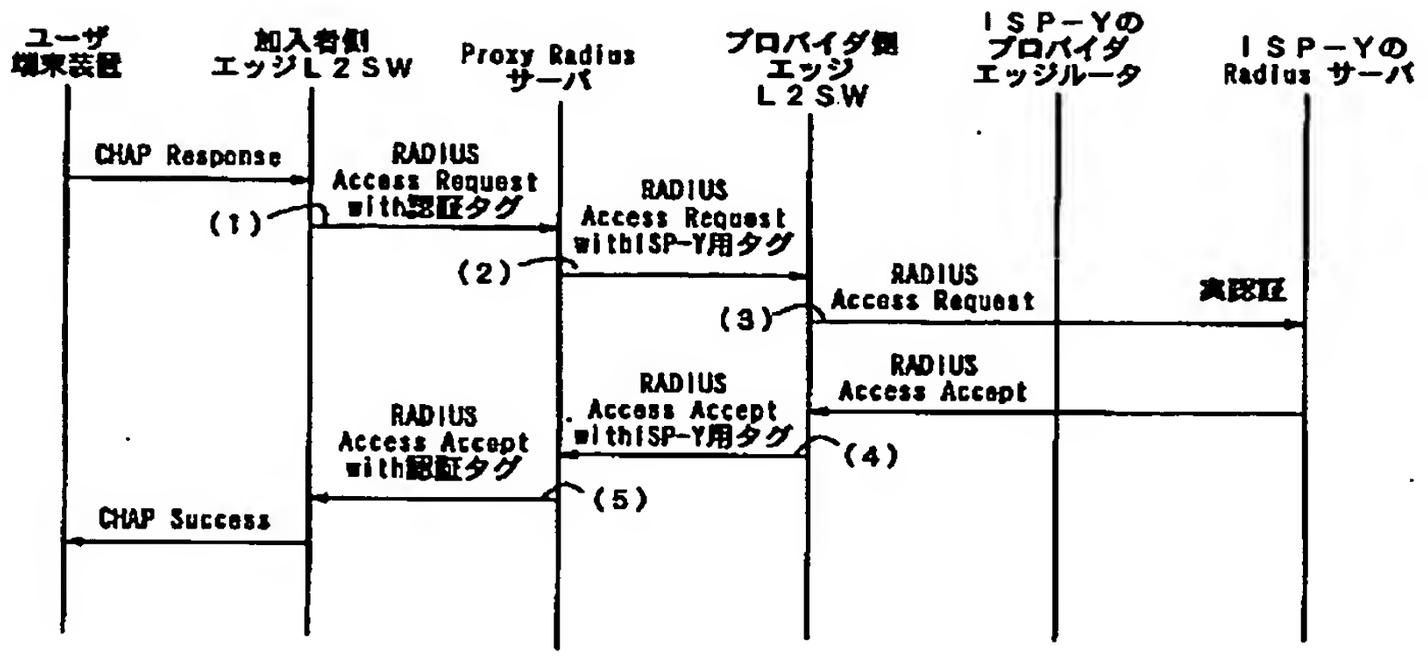
【図36】


プロバイダエッジルータの
MACアドレス／
IPアドレスは固定
30
51 プロバイダ
エッジルータ
52 プロバイダ
Radiusサーバ
6 アクセス網
1
2
3
4
6
6
7
プロバイダ側エッジL2SW
ISP-X
MACアドレス：x
IPアドレス：x
ISP-Y
MACアドレス：y
IPアドレス：y
ISP-Z
MACアドレス：z
IPアドレス：z
プロバイダ毎のポート固定
1台にすべてのプロバイダが
接続されるとは限らない

【図39】

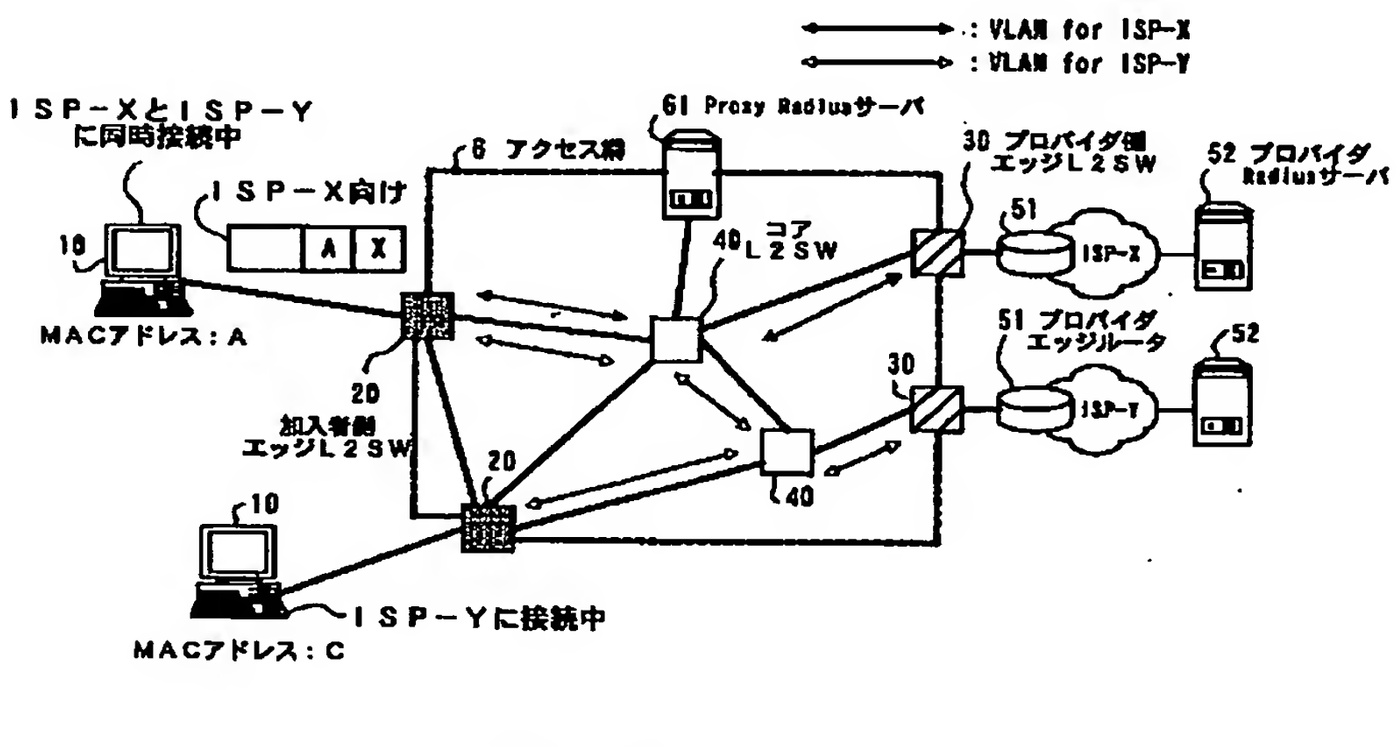

Radius Access-Request
UDP IP 100 Ether
61
ユーザ名●プロバイダ名から
対応するRadius サーバに送信
UDP IP 10 Ether
10
20
40
51
52
A
A,C
B
C
UDP IP 100 Ether
UDP IP 11 Ether
VLAN-ID Attribute追加
Ether 100 IP UDP
Radius Access-Accept
Ether 10 IP UDP
受信したVLAN-ID値により
VLAN-IDテーブル登録
Ether 100 IP UDP
Ether 11 IP UDP
A：管理VLAN (VLAN-ID=100)
B：VLAN for ISP-X (VLAN-ID=10)
C：VLAN for ISP-Y (VLAN-ID=11)

【図41】




（1）認証タグを付加してProxy Radiusサーバに送信
（2）接続先プロバイダを識別、対応するタグに付け替えて転送
（3）タグ除去
（4）入力ポートよりＩＳＰ－Ｙ用タグを付加
（5）ＩＳＰ－Ｙに対応するタグＩＤ値を属性として追加して転送

【図43】




【図44】

| MACアドレス | セッションーＩＤ | VLAN-ＩＤ |
|---|---|---|
| A | 0x1234 | 10 |
| A | 0x5678 | 11 |
| | 0x7777 | |
| C | 0x3859 | 11 |

送信元ＭＡＣアドレスだけで
ＶＩＤテーブルを引くと複数
ＶＬＡＮにマッチしてしまう

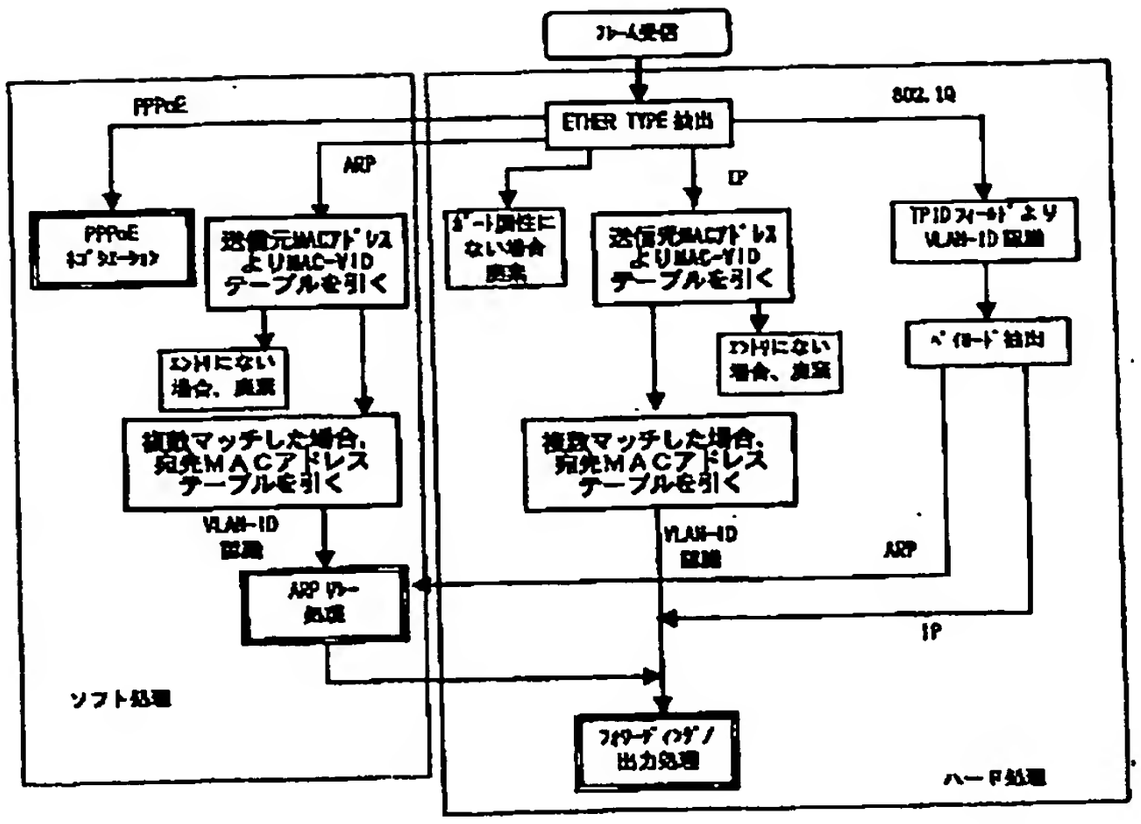
複数同時接続時のＭＡＣ－ＶＩＤテーブル

| 宛先MACアドレス | VLAN-ＩＤ |
|---|---|
| X | 10 |
| Y | 11 |

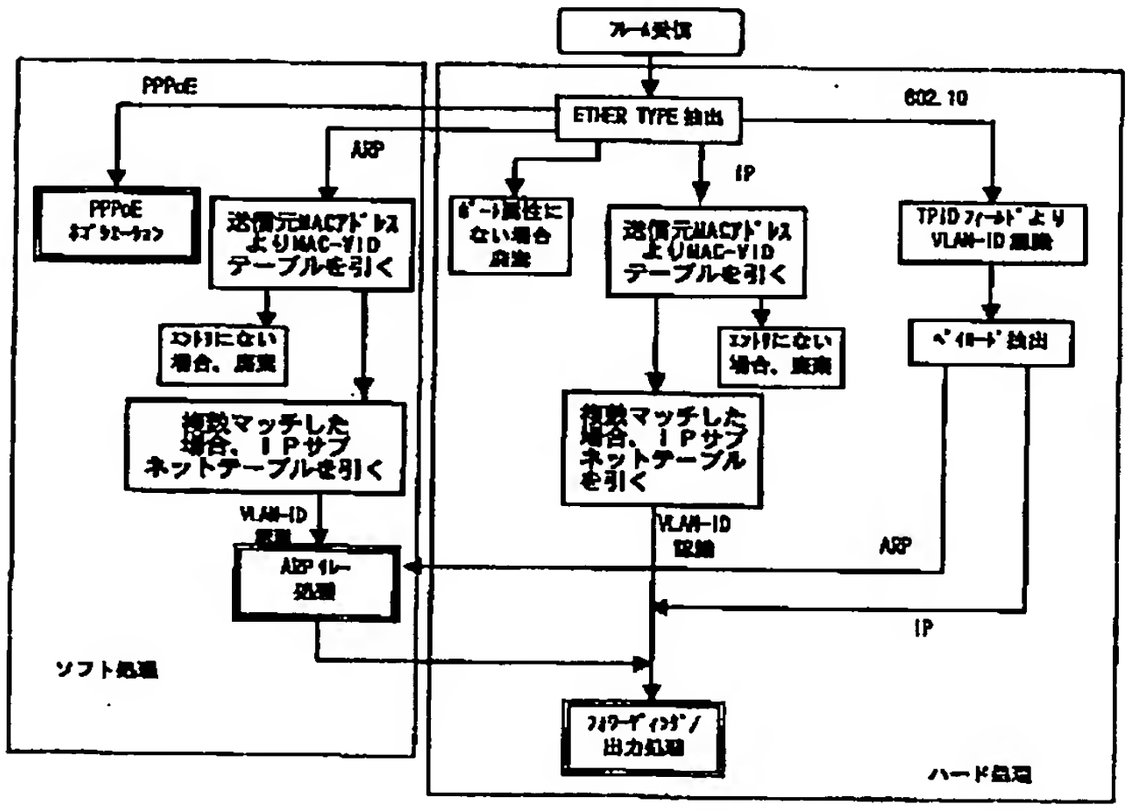
→ 宛先ＭＡＣアドレスにより
ＶＬＡＮ-ＩＤ＝１０と識別

宛先ＭＡＣアドレステーブル
（ＡＲＰリプライをもとに作成）

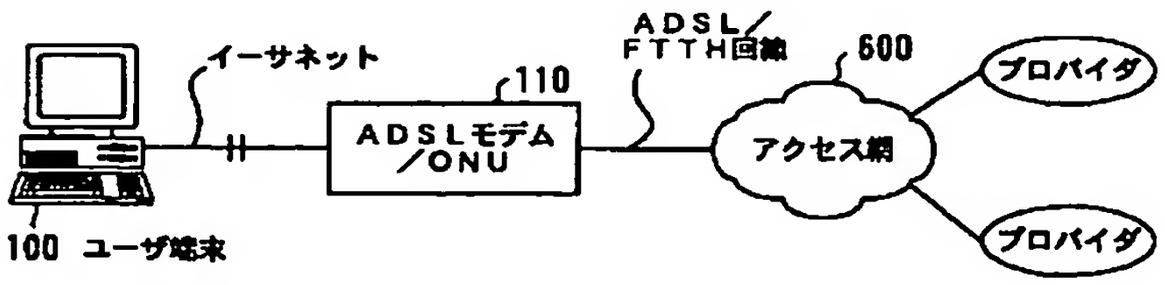
【図45】


フレーム受信
PPPoE
ETHER TYPE 抽出
802.1Q
ARP
IP
PPPoE
ディスカバリー
送信元MACアドレス
よりMAC-VID
テーブルを引く
ポート属性に
ない場合
廃棄
送信元MACアドレス
よりMAC-VID
テーブルを引く
TPIDフィールドより
VLAN-ID 抽出
エントリにない
場合、廃棄
エントリにない
場合、廃棄
ペイロード抽出
複数マッチした場合、
宛先MACアドレス
テーブルを引く
複数マッチした場合、
宛先MACアドレス
テーブルを引く
VLAN-ID
抽出
VLAN-ID
抽出
ARP
ARP リレー
処理
IP
ソフト処理
フォワーディング/
出力処理
ハード処理

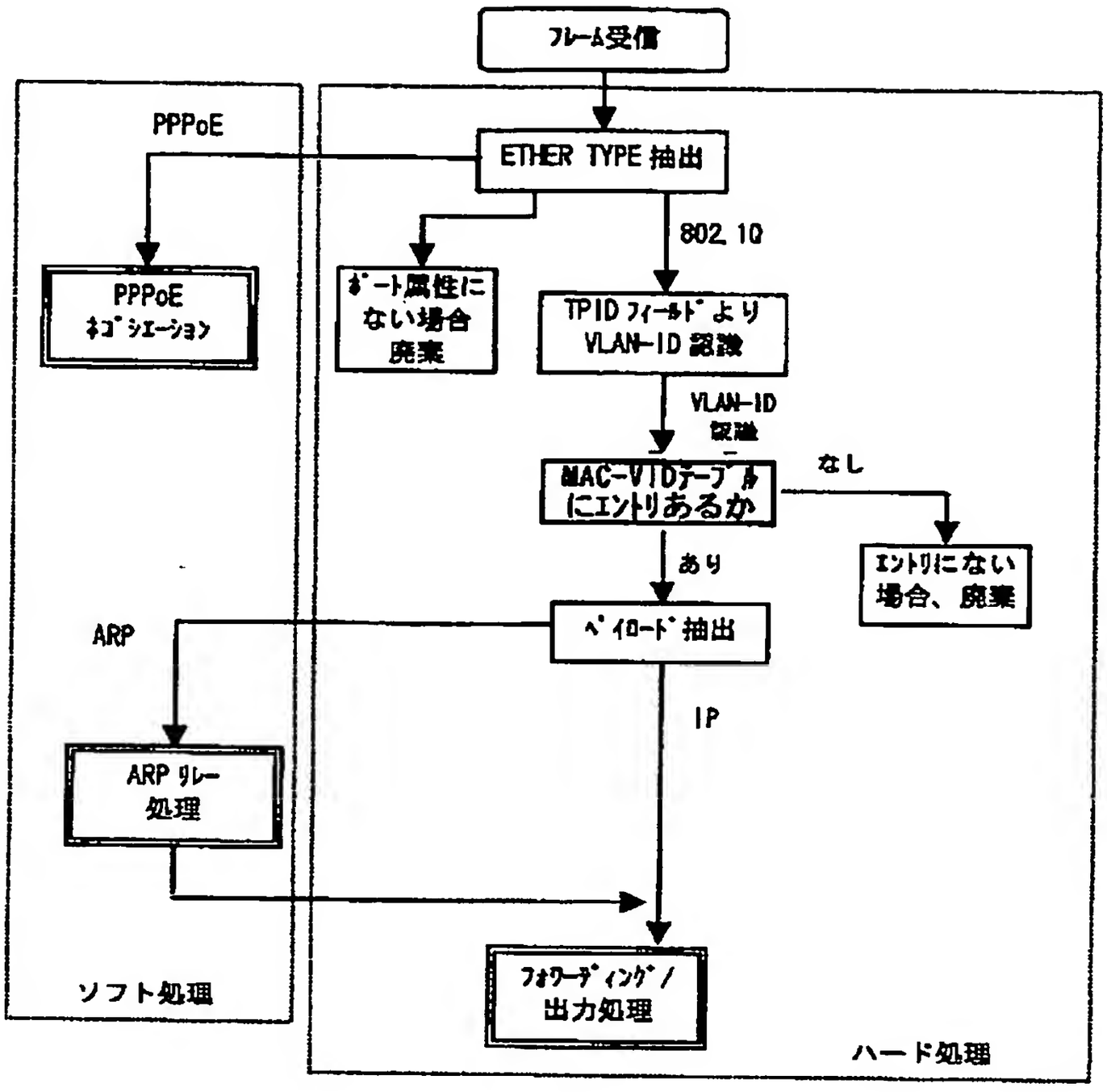
【図48】


フレーム受信
PPPoE
ETHER TYPE 抽出
802.1Q
ARP
IP
PPPoE
ディスカバリー
送信元MACアドレス
よりMAC-VID
テーブルを引く
ポート属性に
ない場合
廃棄
送信元MACアドレス
よりMAC-VID
テーブルを引く
TPIDフィールドより
VLAN-ID 抽出
エントリにない
場合、廃棄
エントリにない
場合、廃棄
ペイロード抽出
複数マッチした
場合、IPサブ
ネットテーブルを引く
複数マッチした
場合、IPサブ
ネットテーブル
を引く
VLAN-ID
抽出
VLAN-ID
抽出
ARP
ARP リレー
処理
IP
ソフト処理
フォワーディング/
出力処理
ハード処理

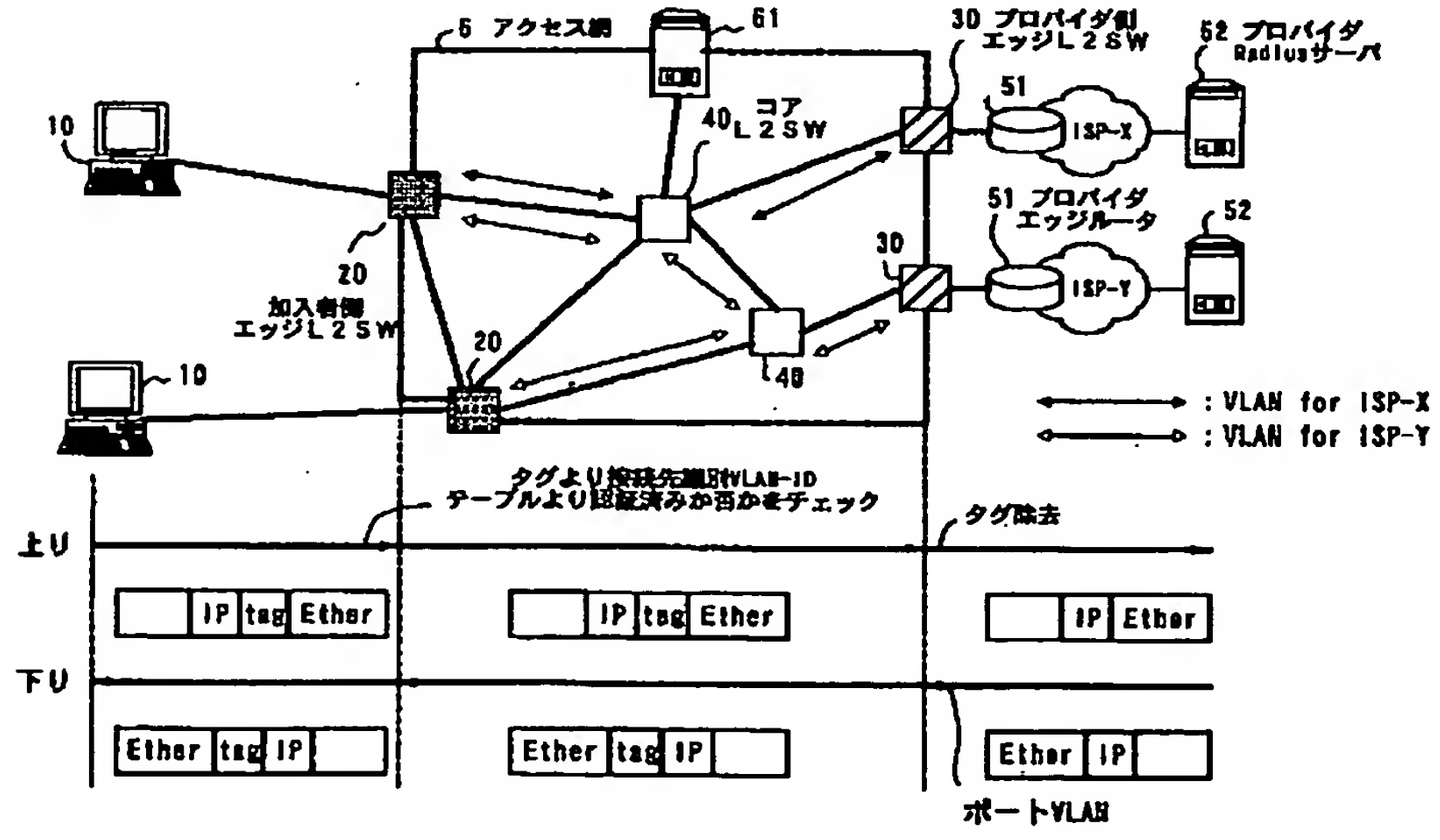
【図65】


イーサネット
110
ADSL/
FTTH回線
600
ADSLモデム
/ONU
アクセス網
プロバイダ
プロバイダ
100 ユーザ端末

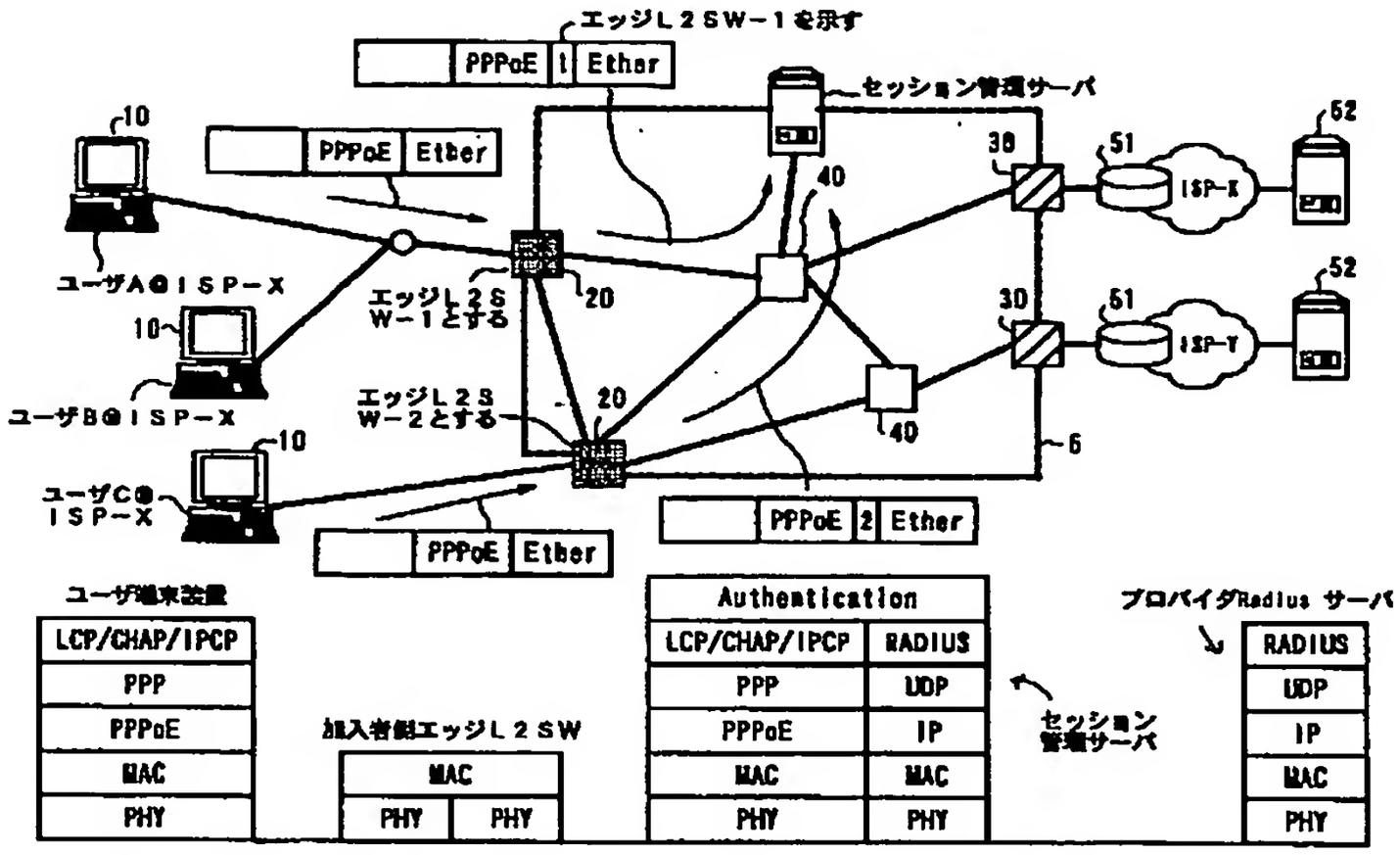
【図49】


フレーム受信
PPPoE
ETHER TYPE 抽出
802.1Q
PPPoE
ネゴシエーション
ポート属性にない場合
廃棄
TPIDフィールドより
VLAN-ID認識
VLAN-ID
認識
MAC-VIDテーブルにエントリあるか
なし
エントリにない場合、廃棄
あり
ペイロード抽出
ARP
IP
ARPリレー
処理
フォワーディング/
出力処理
ソフト処理
ハード処理

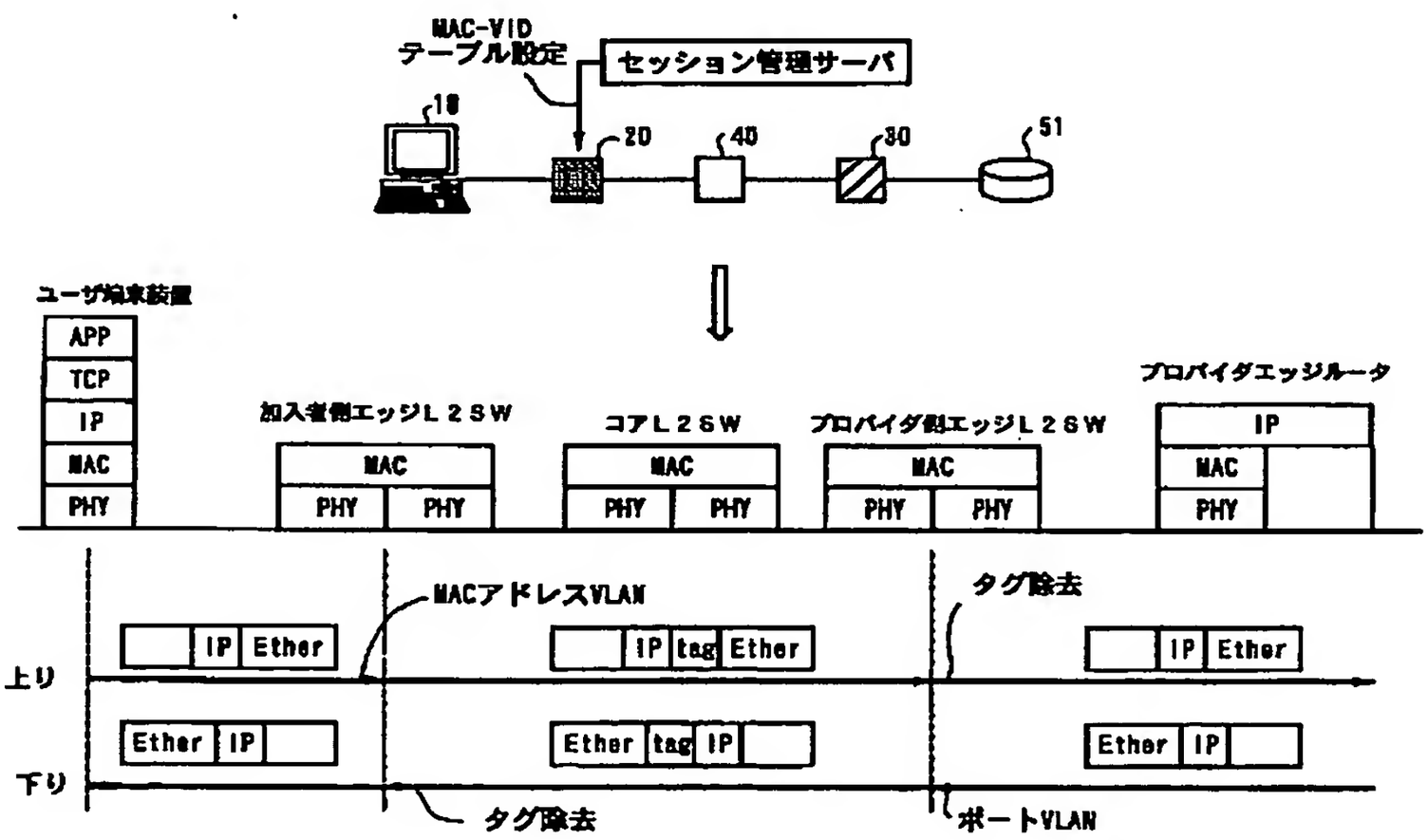
【図50】


5 アクセス網
61
30 プロバイダ側
エッジL2SW
52 プロバイダ
Radiusサーバ
51
ISP-X
40 コア
L2SW
10
51 プロバイダ
エッジルータ
52
30
ISP-Y
20
加入者側
エッジL2SW
20
48
10
: VLAN for ISP-X
: VLAN for ISP-Y
タグより被扱先識別VLAN-ID
テーブルより認証済みか否かをチェック
タグ除去
上り
IP tag Ether
IP tag Ether
IP Ether
下り
Ether tag IP
Ether tag IP
Ether IP
ポートVLAN

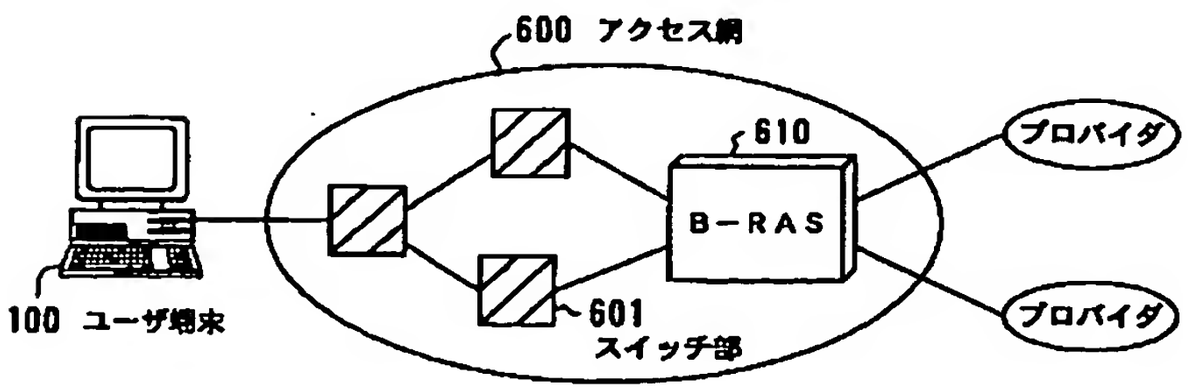
【図51】


エッジL2SW-1を示す
PPPoE
1
Ether
セッション管理サーバ
10
PPPoE
Ether
40
30
51
ISP-X
52
ユーザA@ISP-X
エッジL2S W-1とする
20
10
ISP-Y
ユーザB@ISP-X
エッジL2S W-2とする
20
40
6
10
ユーザC@ISP-X
PPPoE
2
Ether
PPPoE
Ether
ユーザ端末装置
LCP/CHAP/IPCP
PPP
PPPoE
MAC
PHY
加入者側エッジL2SW
MAC
PHY
PHY
Authentication
LCP/CHAP/IPCP
PPP
PPPoE
MAC
PHY
RADIUS
UDP
IP
MAC
PHY
プロバイダRadius サーバ
RADIUS
UDP
IP
MAC
PHY
セッション管理サーバ

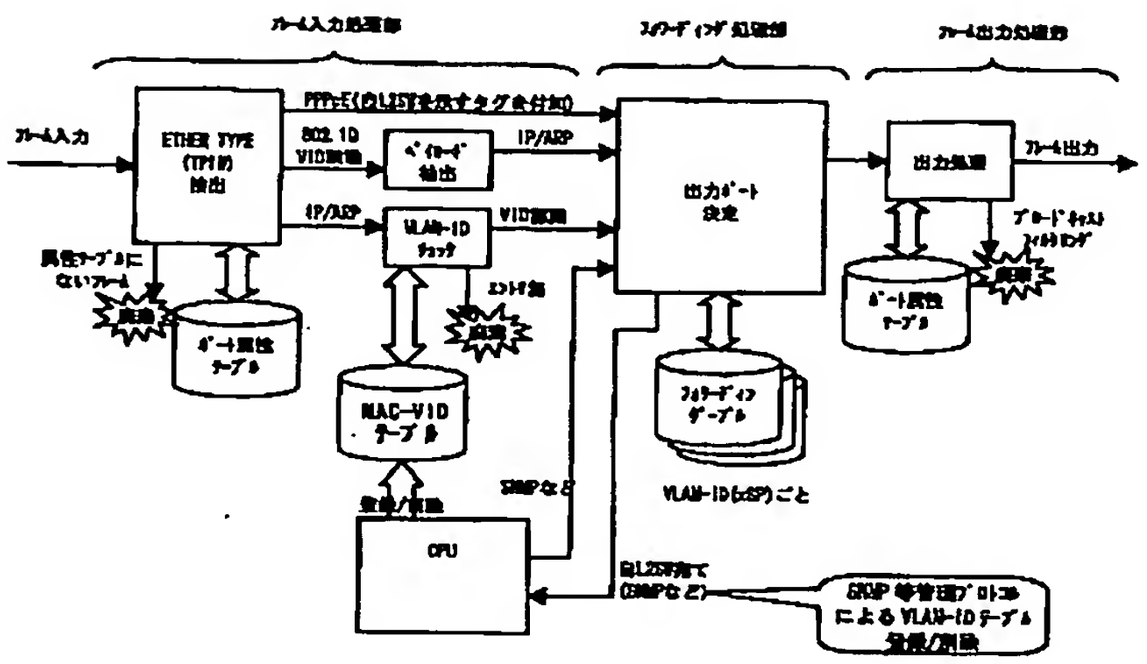
【図52】


MAC-VID テーブル設定
セッション管理サーバ
10
20
40
30
51
ユーザ端末装置
APP
TCP
IP
MAC
PHY
加入者側エッジL2SW
MAC
PHY
PHY
コアL2SW
MAC
PHY
PHY
プロバイダ側エッジL2SW
MAC
PHY
PHY
プロバイダエッジルータ
IP
MAC
PHY
MACアドレスVLAN
タグ除去
IP
Ether
IP
tag
Ether
上り
下り
Ether
IP
Ether
tag
IP
タグ除去
ポートVLAN

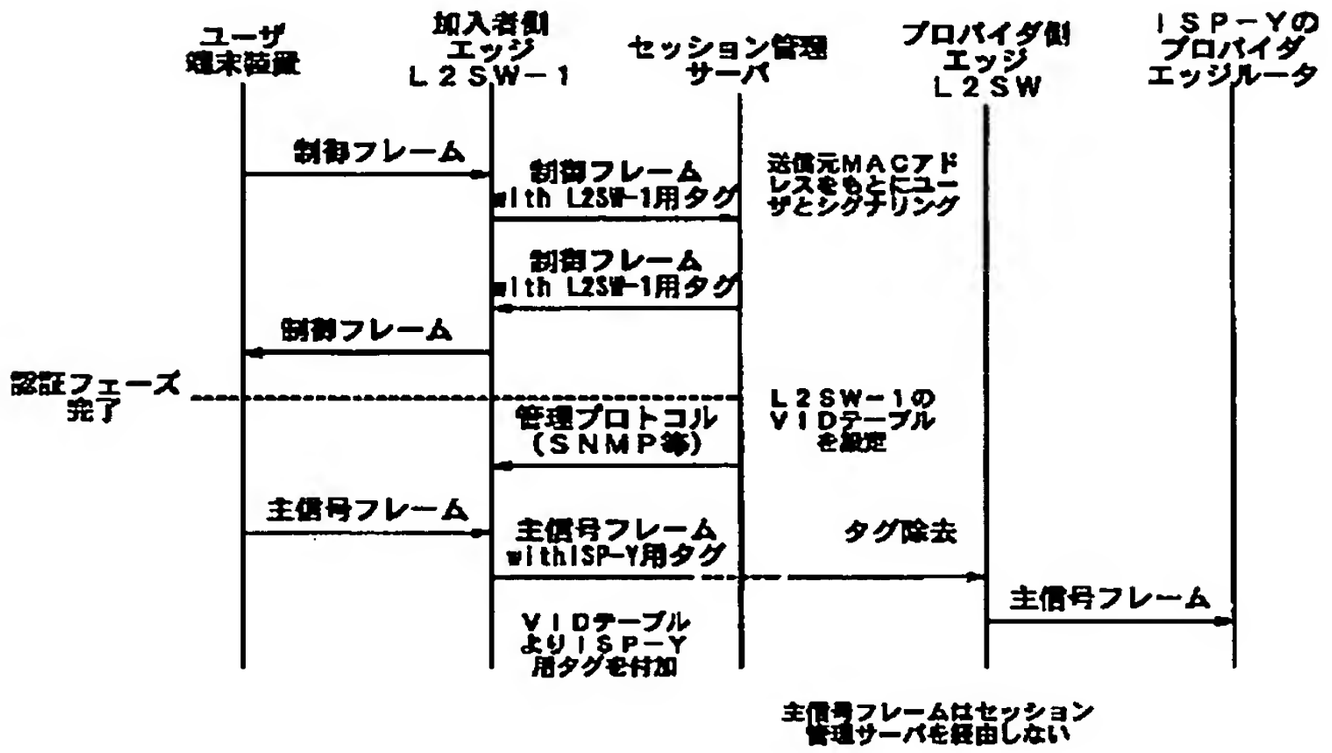
【図66】


600 アクセス網
610
B-RAS
プロバイダ
プロバイダ
100 ユーザ端末
601
スイッチ部

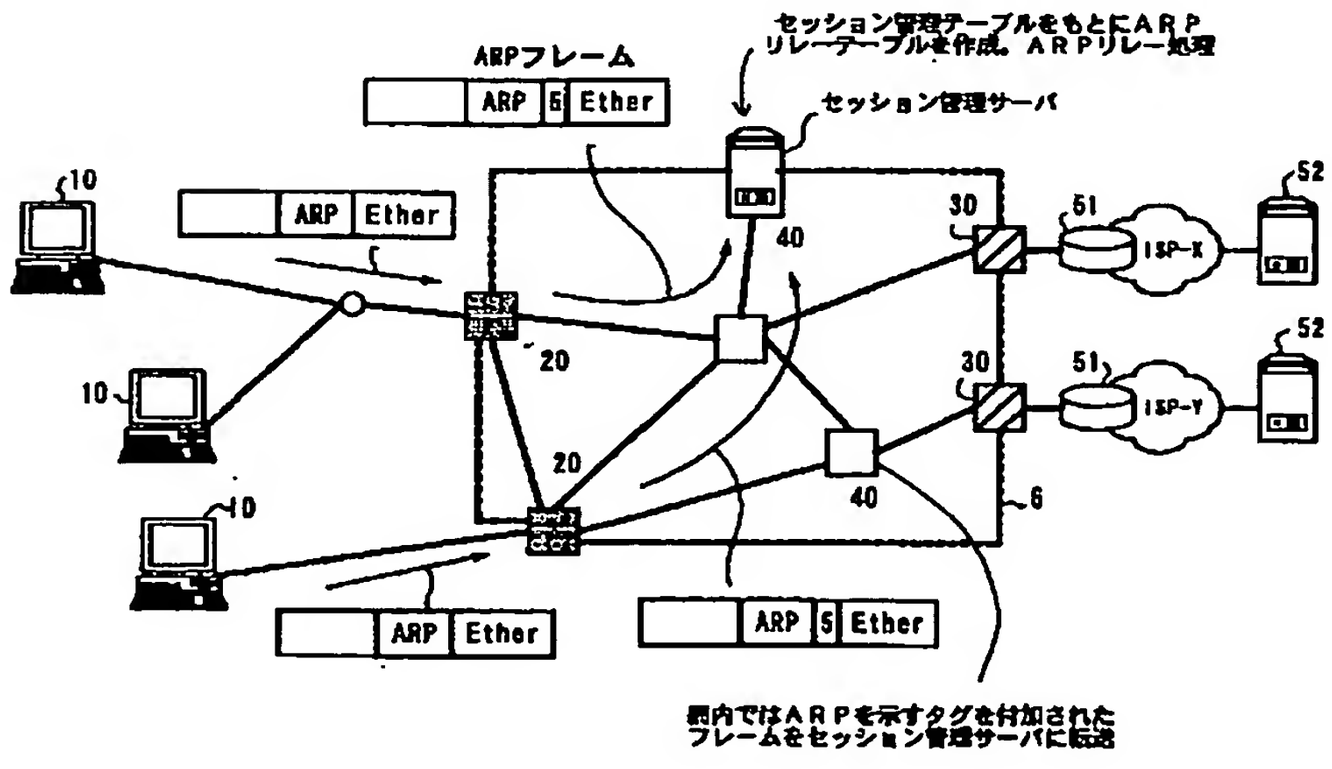
【図53】


ETHER TYPE
(TPID)
検出
802.1Q
VID解釈
ペイロード
抽出
IP/ARP
VLAN-ID
チェック
VID解釈
出力ポート
設定
出力処理
MAC-VID
テーブル
CPU
VLAN-ID(&ISP)ごと
SNMPなど

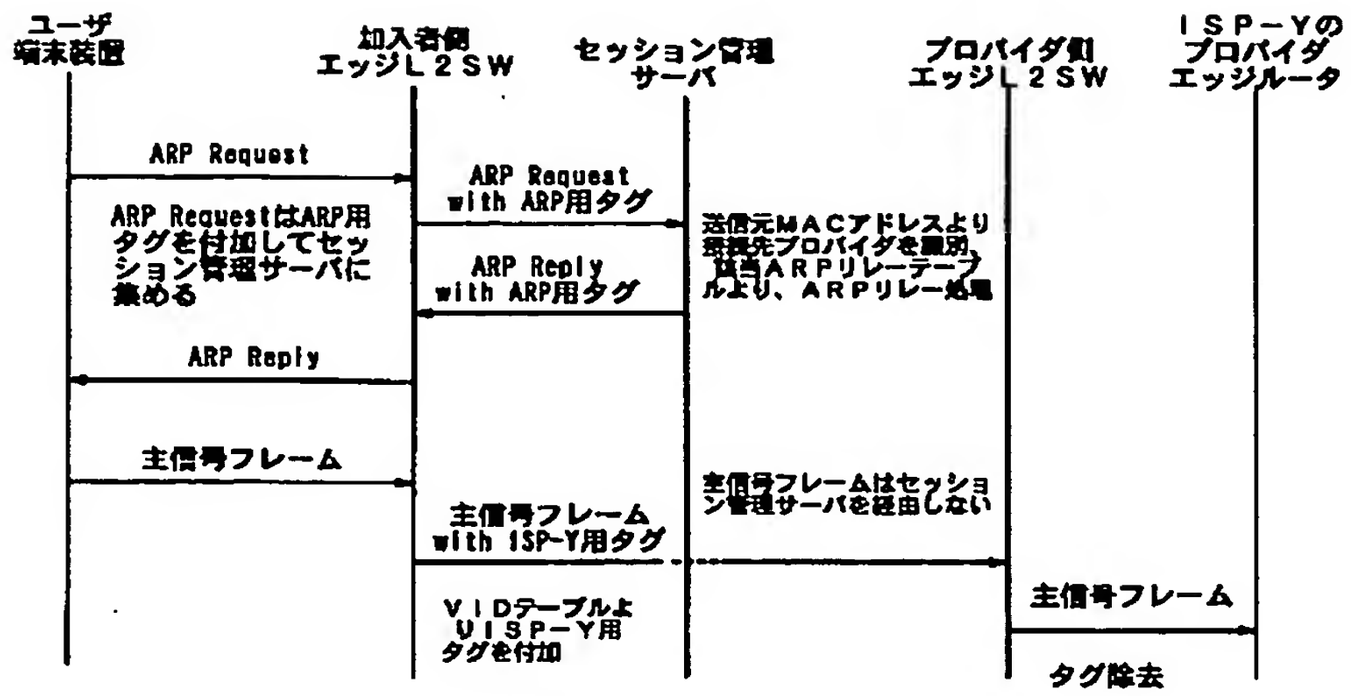
【図54】


ユーザ
端末装置
加入者側
エッジ
L2SW-1
セッション管理
サーバ
プロバイダ側
エッジ
L2SW
ISP-Yの
プロバイダ
エッジルータ
制御フレーム
制御フレーム
with L2SW-1用タグ
送信元MACアドレスをもとにユーザとシグナリング
制御フレーム
with L2SW-1用タグ
制御フレーム
認証フェーズ
完了
L2SW-1のVIDテーブルを設定
管理プロトコル
(SNMP等)
主信号フレーム
主信号フレーム
withISP-Y用タグ
タグ除去
主信号フレーム
VIDテーブルよりISP-Y用タグを付加
主信号フレームはセッション管理サーバを経由しない

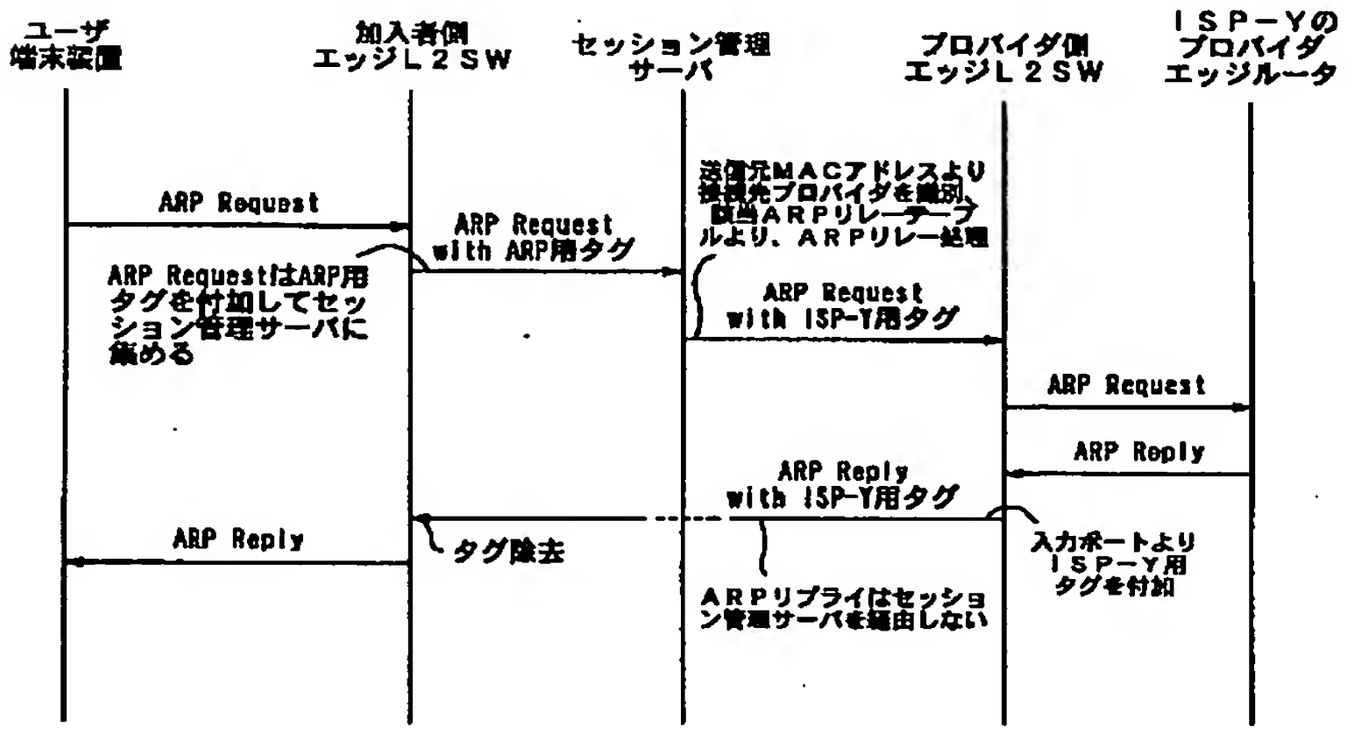
【図55】


セッション管理テーブルをもとにARPリレーテーブルを作成。ARPリレー処理
ARPフレーム
ARP
6
Ether
セッション管理サーバ
10
ARP
Ether
20
30
40
51
ISP-X
52
ISP-Y
6
網内ではARPを示すタグを付加されたフレームをセッション管理サーバに転送

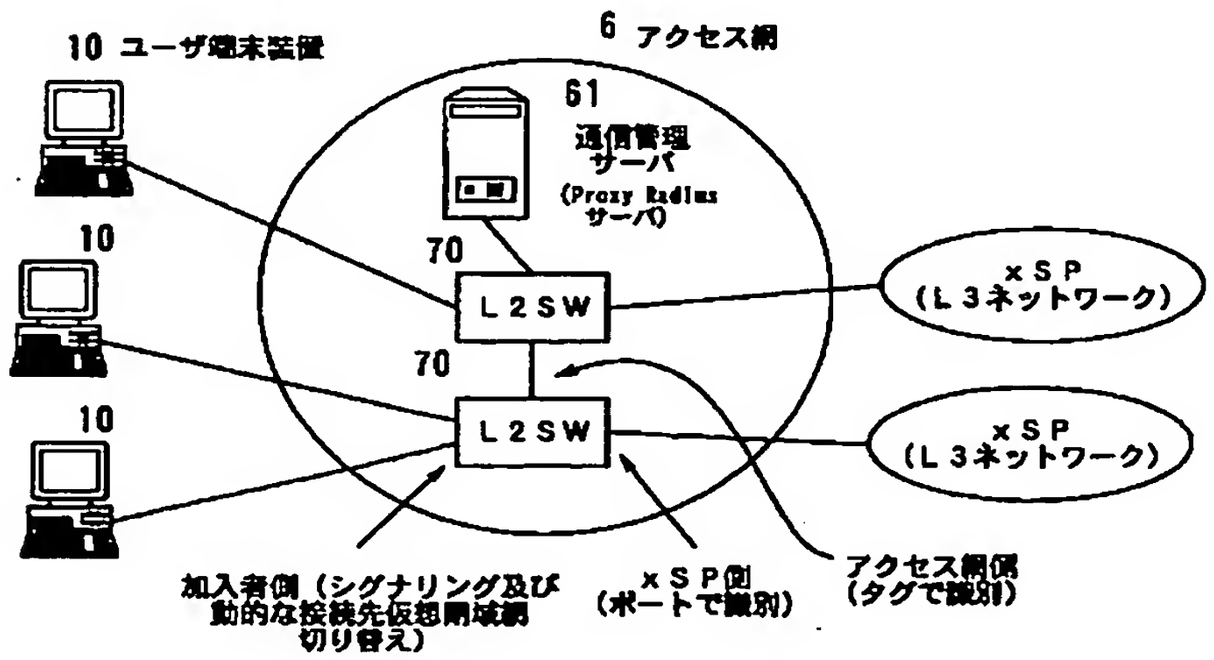
【図56】


ユーザ
端末装置
加入者側
エッジＬ２ＳＷ
セッション管理
サーバ
プロバイダ側
エッジＬ２ＳＷ
ＩＳＰ－Ｙの
プロバイダ
エッジルータ
ARP Request
ARP Request
with ARP用タグ
ARP RequestはARP用
タグを付加してセッ
ション管理サーバに
集める
送信元ＭＡＣアドレスより
接続先プロバイダを識別、
該当ＡＲＰリレーテーブ
ルより、ＡＲＰリレー処理
ARP Reply
with ARP用タグ
ARP Reply
主信号フレーム
主信号フレームはセッション
管理サーバを経由しない
主信号フレーム
with ISP-Y用タグ
主信号フレーム
ＶＩＤテーブルよ
ＵＩＳＰ－Ｙ用
タグを付加
タグ除去

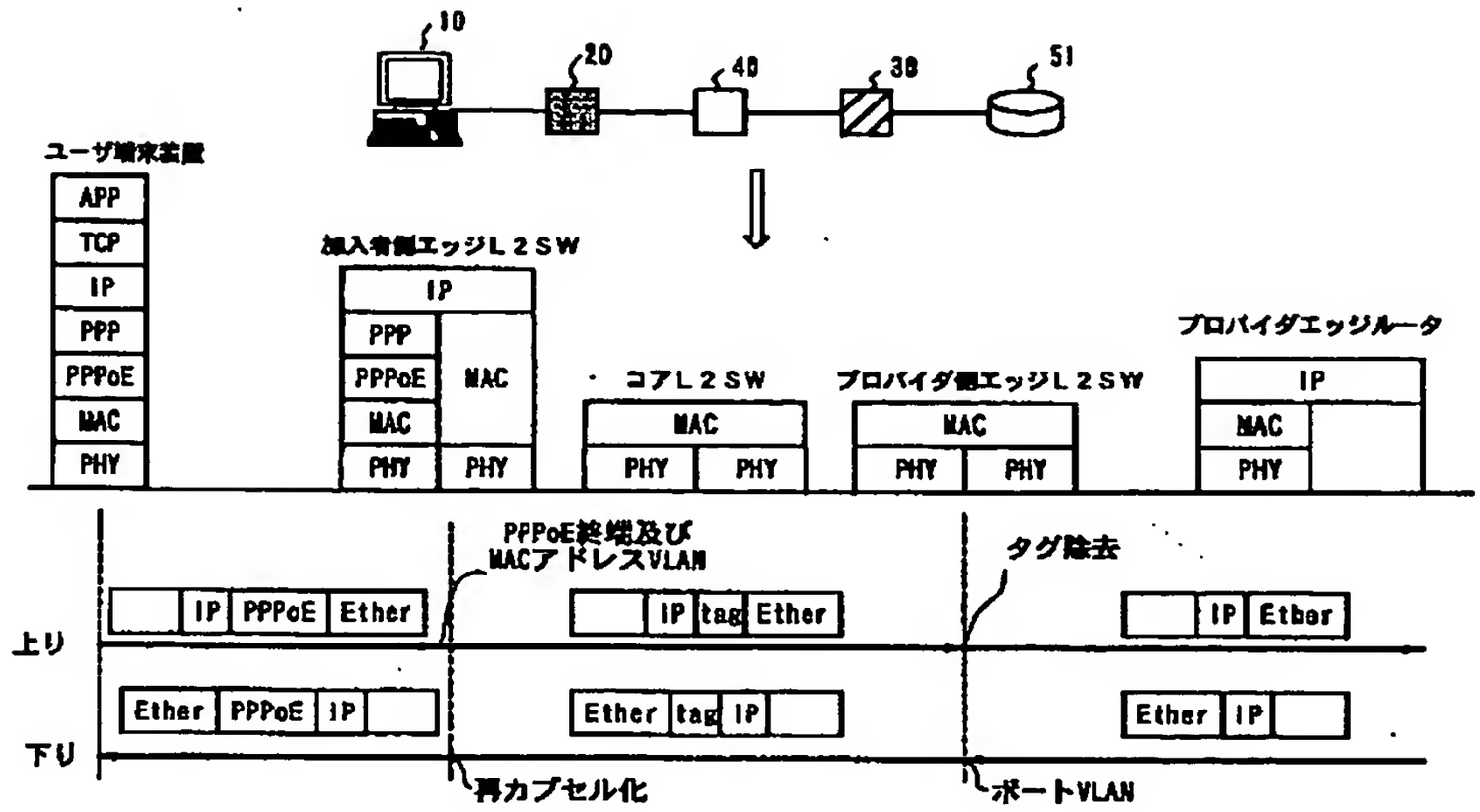
【図57】


ユーザ
端末装置
加入者側
エッジＬ２ＳＷ
セッション管理
サーバ
プロバイダ側
エッジＬ２ＳＷ
ＩＳＰ－Ｙの
プロバイダ
エッジルータ
ARP Request
ARP Request
with ARP用タグ
ARP RequestはARP用
タグを付加してセッ
ション管理サーバに
集める
送信元ＭＡＣアドレスより
接続先プロバイダを識別、
該当ＡＲＰリレーテーブ
ルより、ＡＲＰリレー処理
ARP Request
with ISP-Y用タグ
ARP Request
ARP Reply
ARP Reply
with ISP-Y用タグ
ARP Reply
タグ除去
入力ポートより
ＩＳＰ－Ｙ用
タグを付加
ＡＲＰリプライはセッショ
ン管理サーバを経由しない

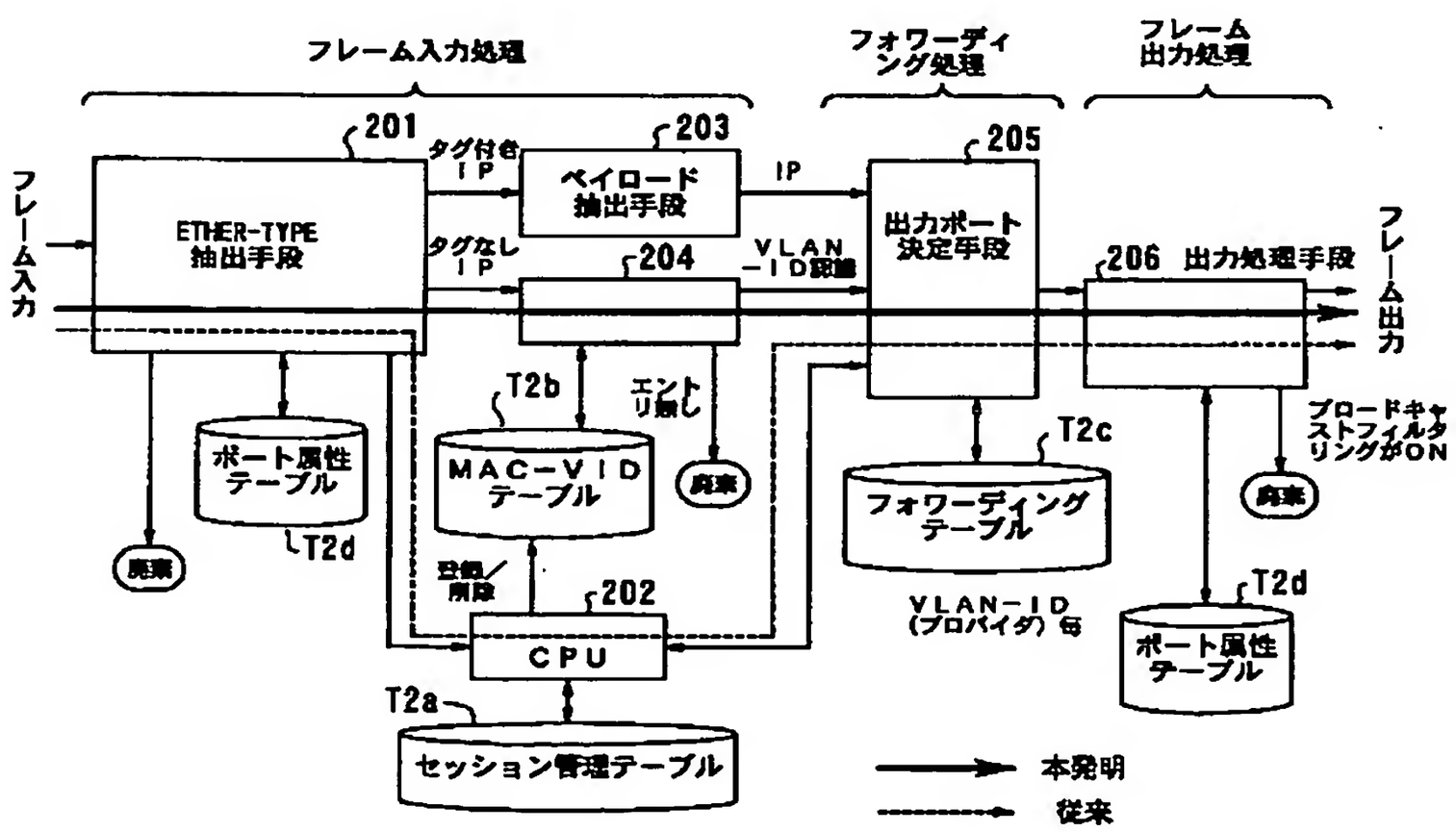
【図60】


1a 通信システム
10 ユーザ端末装置
6 アクセス網
61
通信管理
サーバ
(Proxy Radius
サーバ)
10
70
ｘＳＰ
（Ｌ３ネットワーク）
L2SW
70
10
L2SW
ｘＳＰ
（Ｌ３ネットワーク）
10
加入者側（シグナリング及び
動的な接続先仮想閉域網
切り替え）
ｘＳＰ側
（ポートで識別）
アクセス網側
（タグで識別）

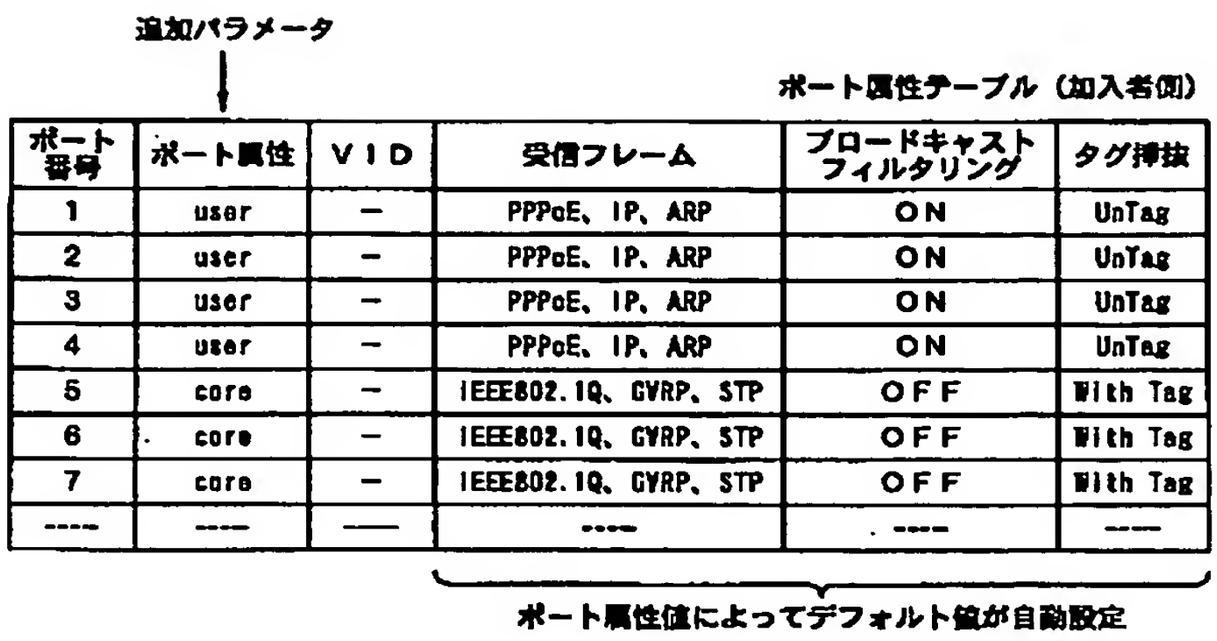
【図58】


10
20
40
38
51
ユーザ端末装置
APP
TCP
IP
PPP
PPPoE
MAC
PHY
加入者側エッジL2SW
IP
PPP
PPPoE
MAC
MAC
PHY
PHY
コアL2SW
MAC
PHY
PHY
プロバイダ側エッジL2SW
MAC
PHY
PHY
プロバイダエッジルータ
IP
MAC
PHY
PPPoE終端及び
MACアドレスVLAN
タグ除去
上り
下り
IP
PPPoE
Ether
IP
tag
Ether
IP
Ether
Ether
PPPoE
IP
Ether
tag
IP
Ether
IP
再カプセル化
ポートVLAN

【図59】

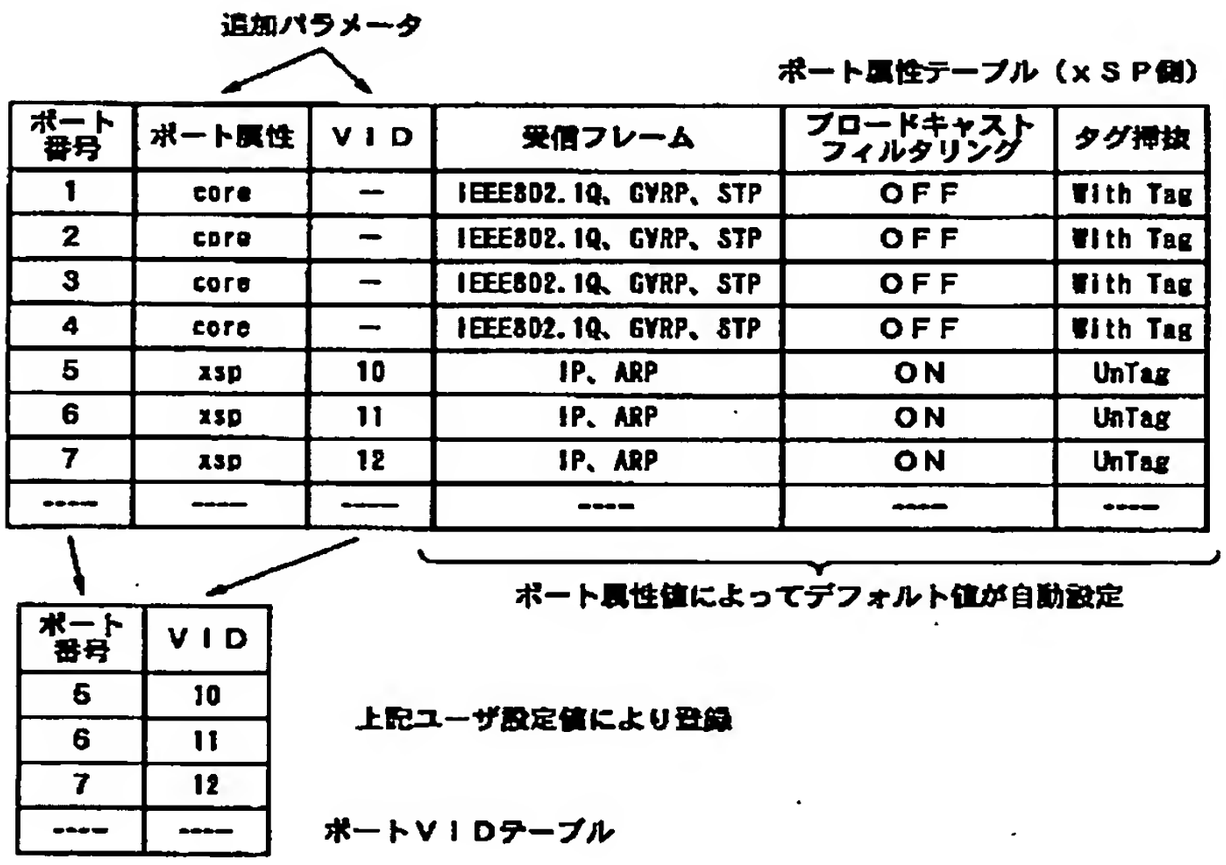

フレーム入力処理
フォワーディング処理
フレーム出力処理
201
203
205
タグ付き IP
タグなし IP
IP
ペイロード抽出手段
ETHER-TYPE抽出手段
VLAN_ID認識
出力ポート決定手段
204
206 出力処理手段
フレーム入力
フレーム出力
T2b
エントリ無し
T2c
ブロードキャストフィルタリングがON
ポート属性テーブル
T2d
MAC-VIDテーブル
廃棄
フォワーディングテーブル
廃棄
廃棄
登録/削除
202
VLAN-ID (プロバイダ) 毎
T2d
ポート属性テーブル
CPU
T2a
セッション管理テーブル
本発明
従来

【図61】




| ポート番号 | ポート属性 | VID | 受信フレーム | ブロードキャストフィルタリング | タグ挿抜 |
|---|---|---|---|---|---|
| 1 | user | — | PPPoE、IP、ARP | ON | UnTag |
| 2 | user | — | PPPoE、IP、ARP | ON | UnTag |
| 3 | user | — | PPPoE、IP、ARP | ON | UnTag |
| 4 | user | — | PPPoE、IP、ARP | ON | UnTag |
| 5 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 6 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 7 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| ---- | ---- | —— | ---- | ---- | ---- |

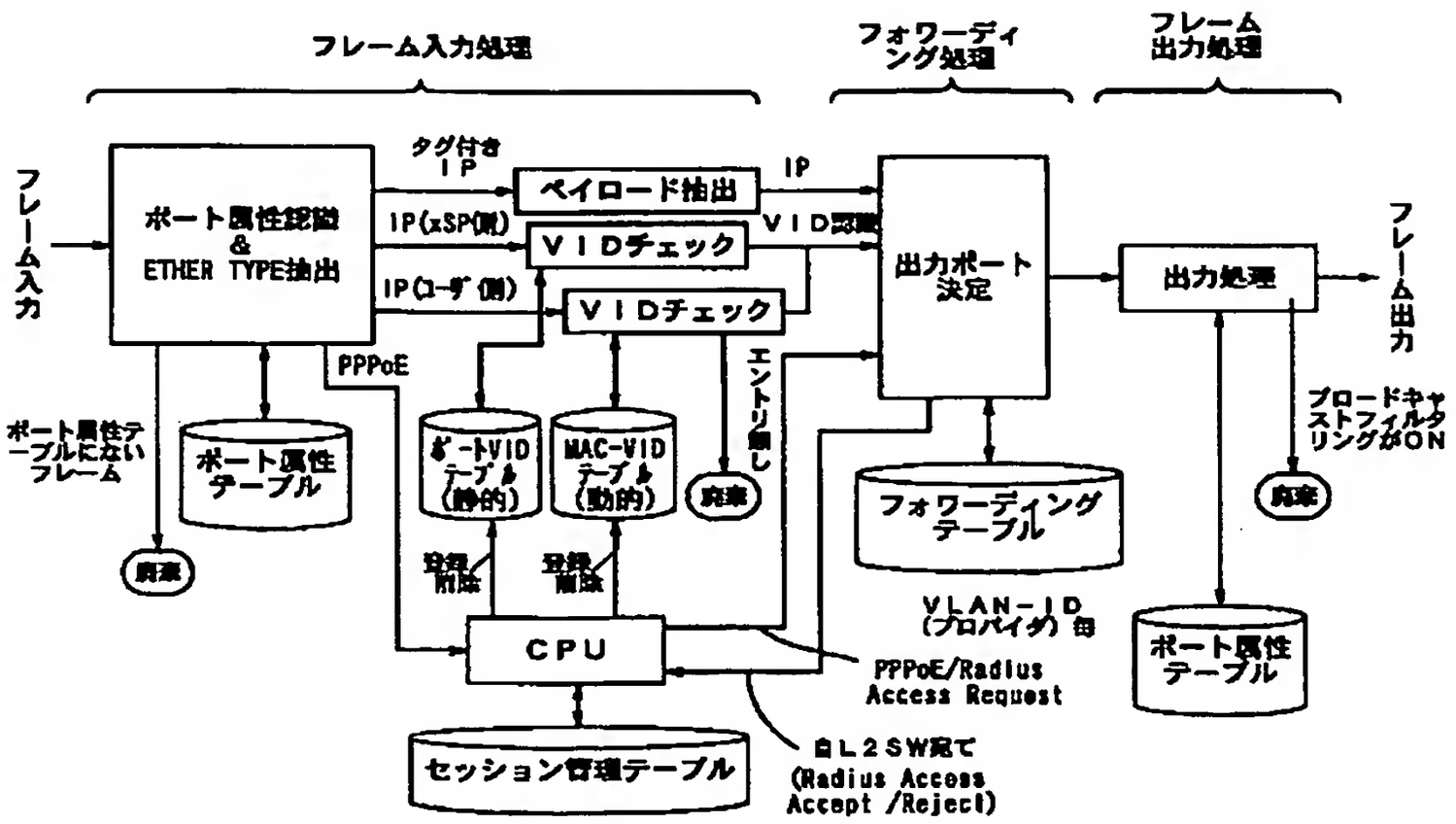
【図62】



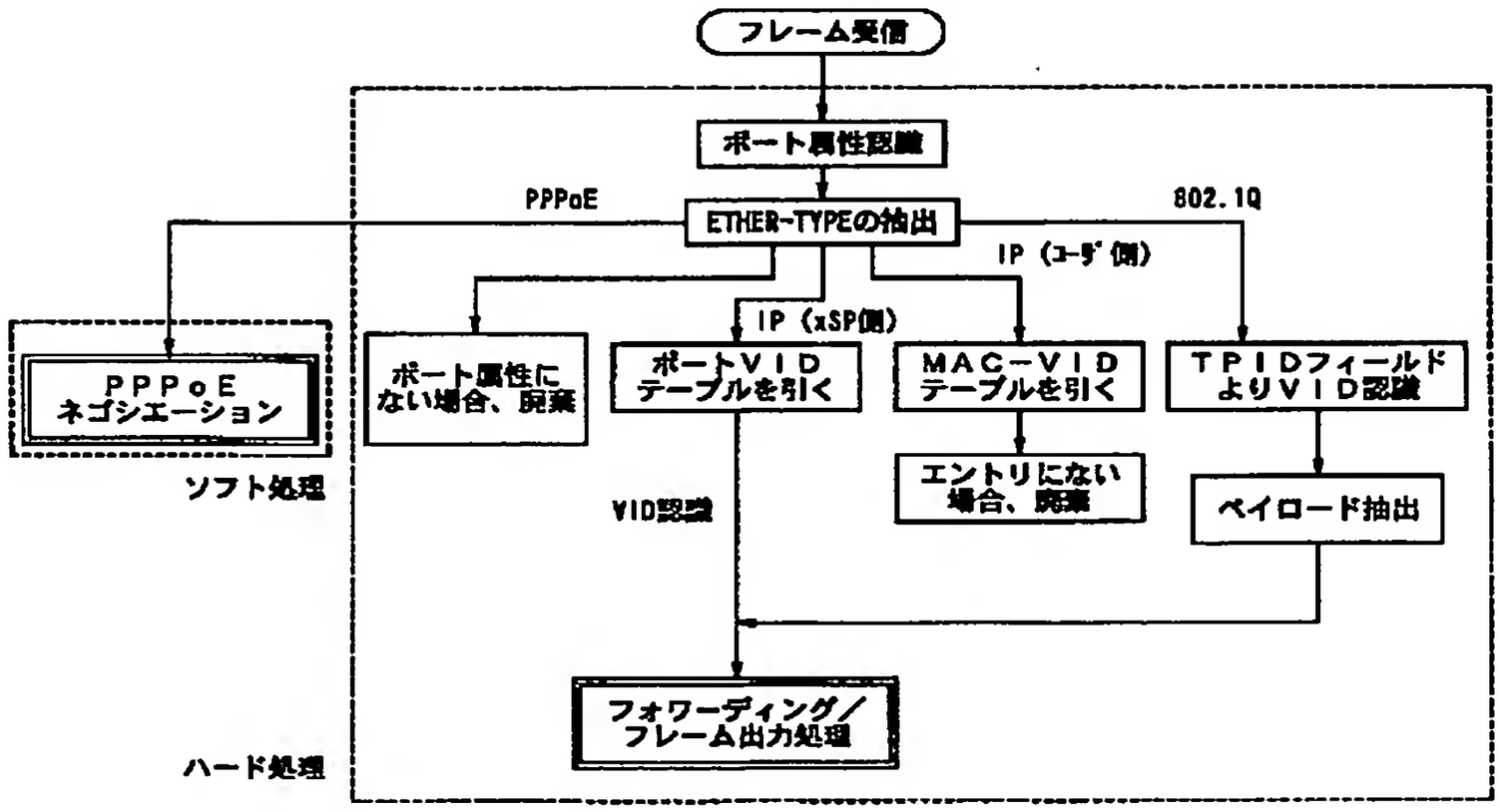

| ポート番号 | ポート属性 | VID | 受信フレーム | ブロードキャストフィルタリング | タグ挿抜 |
|---|---|---|---|---|---|
| 1 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 2 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 3 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 4 | core | — | IEEE802.1Q、GVRP、STP | OFF | With Tag |
| 5 | xsp | 10 | IP、ARP | ON | UnTag |
| 6 | xsp | 11 | IP、ARP | ON | UnTag |
| 7 | xsp | 12 | IP、ARP | ON | UnTag |
| ---- | ---- | —— | ---- | ---- | ---- |

| ポート番号 | VID |
|---|---|
| 5 | 10 |
| 6 | 11 |
| 7 | 12 |
| ---- | ---- |

【図63】




【図64】




---

フロントページの続き

Fターム(参考) 5K030 HA08 HC01 HC13 HD08 HD09
5K033 AA08 CB01 CB02 CB08 DA05
EC03
5K034 AA05 DD02 EE10 LL01